Signamax™ Connectivity Systems

Analogue Telephone Adapter 065-9055/065-9056

Wi-Fi Analogue Telephone Adapter 065-9061/065-9062

For SIP

User's Manual

Version 1.14

Table of Contents

TABLE OF CONTENTS 2

PREFACES 5

0.1 About This Manual 5
0.2 Copyright Declarations 5
0.3 Trademarks 5
0.4 Safety Instructions 5
0.5 Warranty 5

INTRODUCE 6

1.1 Overview 6
1.2 Audience 6
1.3 Acronyms Table 6
1.4 Introduction 7
1.5 Front Panel LED Indicators & Rear Panels 7
1.6 ATA / Wifi Specification 8
VoIP Key Features: 8
Telephony Specification: 8
IP Specification: 9
Call Features: 9
Configuration & Management: 9
General Specification: 9
Wireless LAN: 9

INSTALLATION AND SETUP 10

2.1 Package Content 10
2.2Hardware Installation 11
Port Description: DEMO Model 065-9055/065-9062 11
Installation: 12
2.3Quick Start 14
2.4 Wizard Setup 14
WAN Port Type Setup: 14
NAT setting: 17
VoIP Call Setup 20

NETWORK SETTING 21

3.1 WAN Setting 21
Static IP 22
DHCP 23
PPPoE 23
Host Name 23
WAN Port MAC 24

MTU and MRU 24
DNS Server 24
Ping From WAN 25
3.2 LAN Setting 25
DNS Proxy 25
3.3 Wlan Setting(Only 065-9061/065-9062 module) 25
3.4 DHCP Server Setting 27
3.5 Static Router 28
3.6 NAT 29
NAT Setting 29
Virtual Server Setting 30
Port Trigger 31
3.7 Packet Filter 31
3.8 URL Filter 32
3.9 Security 33
3.10 UPNP 34
3.11 DDNS 34
3.12 SNMP 35

SIP SETTING 36

4.1 Basic Setting 37
4.2 Account Setting 39
4.3 Server Setting 40
4.4 NAT Travertal 40

VOIP SETTING 41

5.1 Voice Setting 42
Codec 42
Voice Active Detecto 43
Echo Canceller 43
Gain Control Level 44
DTMF Method 44
RTP 44
5.2 Call Service 45
Call Waiting 45
Call Transfer Option 46
Call Forward Option 46
5.3 FXS Port Setting 47
5.4 FXO Port Setting 48
5.5 FAX Setting 49
5.6 General Dialing Setting 50
5.7 Phone Book 50
5.8 IP Call table 51
5.9 Call Screen 52
5.10 QOS Setting 52

INFORMATION 53

6.1 System Information 53
6.2 Line Status 54

MANAGEMENT..... 54

7.1 Administrator Account 55
7.2 Date/time 55
7.3 Ping Test 56
7.4 Save/Restore 56
7.5 Factory Default 57
7.6 Firmware Update 57
7.7 Auto provision 57
7.8 Check network alive 58

SAVE & LOGOUT 59

8.1 Save 59
8.2 Save & Logout 59
8.3 Save & Reboot 59

APPENDIX..... 59

A - FAQ List 59
B - Scenario Application Samples 61

Prefaces

0.1 About This Manual

This manual is designed to assist users in using Analogue Telephone Adapter (ATA) or Wi-Fi Analogue Telephone Adapter (ATA). Information in this document has been carefully checked for accuracy; however, no guarantee is given as to the correctness of the contents. The information contained in this document is subject to change without notice.

0.2 Copyright Declarations

Copyright 2006 Telephony Corporation. All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.

0.3 Trademarks

Products and Corporate names appearing in this manual may or not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owners' benefit, without to infringe.

0.4 Safety Instructions

The most careful attention has been devoted to quality standards in the manufacture of the Analogue Telephone Adapter (ATA) or Wi-Fi Analogue Telephone Adapter (ATA). Safety is a major factor in the design of every set. But, safety is your responsibility too.

- Use only the required power voltage. Power Input: AC 110V/220V, 50-60Hz
- To reduce the risk of electric shock, do not disassemble this product. Opening or removing covers may expose the ATA to hazardous voltages. Incorrect reassembly can cause electric shock when this product is subsequently used.
- Never push objects of any kind into the equipment through housing slots since they may touch hazardous voltage points or short out parts those could result in a risk of electric shock. Never spill liquid of any kind on the product. If liquid is spilled, please refer to the proper service personnel.
- Use only Unshielded Twisted Pair (UTP) Category 5 Ethernet cable to RJ-45 port of the Analogue Telephone Adapter (ATA).

0.5 Warranty

We warrant to the original end user (purchaser) that the SA series Analogue Telephone Adapter (ATA) will be free from any defects in workmanship or materials for a period of one (1) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary to re-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of

merchantability or fitness for a particular use or purpose. We shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact us for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by us to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Introduce

065-9055/065-9056 series are the low cost Void Solutions. This document describes the usage of ATA (Analogue Telephone Adapter)

1.1 Overview

- An Analogue Telephone Adapter, or ATA, is a device that allows one to connect a normal PSTN telephone to the Internet in order to make or place telephone calls.
- ATA provides a direct analog interface for PSTN, PBX, fax machines, analog telephones, and other devices that require an analog port.
- With a built-in IEEE 802.11b/g wireless AP, the Wi-Fi ATA offers maximum mobility via 54Mbps data transmissions.

1.2 Audience

This document is intended for system vendor who are using ATA or Wi-Fi ATA to build an Internet telephony gateway or server application. It is assumed that the reader has the general knowledge of VoIP applications and products.

1.3 Acronyms Table

Acronym:	Full Name:	Acronym:	Full Name:
API	Application Interface	ACI	Audio CODEC Interface
ADC	Analog to Digital Converter	CODEC	Coder / Decoder
DAC	Digital to Analog Converter	DC	Direct Current
DDNS	Dynamic Domain Name System	DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone	DNS	Domain Name System
DTMF	Dual Tone Multi Frequency	FXO	Foreign Exchange Office
FXS	Foreign Exchange Station	GMT	Greenwich Mean Time
IP	Internet Protocol	IPsec	Internet Protocol Security
L2TP	The Layer 2 Tunnel Protocol	LAN	Local Area Network
WAN	Wide Area Network	MAC	Media Access Control
MII	Media Independent Interface	NAT	Network Address Translation
NTP	Network Time Protocol	PPTP	Point-to-Point Tunneling Protocol
RTP	Real-Time Transport Protocol	RTCP	Real-Time Transport Control Protocol (also known as RTP control protocol)
SIP	Session Initiation Protocol	SLIC	Subscriber Line Interface Circuit
STUN	Simple Traversal of UDP through NATs	URI	Uniform Resource Identifier
TCP	Transmission Control Protocol	UDP	User Datagram Protocol
UPnP	Universal Plug and Play	VoIP	Voice Over Internet Protocol

1.4 Introduction

This Analogue Telephone Adapter (ATA) provides a total solution for integrating voice-data network and PSTN.

The 065-9055/065-9056 Analogue Telephone Adapter (ATA) support SIP VoIP Protocol. **The 065-9055/065-9056** Analogue Telephone Adapter (ATA) allows 1~2 lines analog voice and fax communication over a traditional data communications/data networking digital Internet.

065-9062/065-9061 is high performance Wireless Router + VoIP gateway that provides small and medium-size offices with faster wireless internet access and VoIP service.

Model	FXO Port	FXS Port	PSTN	WAN Port	LAN Port	RJ-11 port	802.11 b/g	SIP
065-9055	0	1	1	1	1	2		√
065-9056	0	2	0	1	1	2		√
065-9061	0	1	1	1	1	2	√	√
065-9062	0	2	0	1	1	2	√	√

1.5 Front Panel LED Indicators & Rear Panels

065-9055 /065-9056

LED	State	Description
1. POWER	On	ATA is power ON
	Off	ATA is power Off
2. LAN port	On	LAN is connected successfully
	Flashing	Data is transmitting
	Off	Ethernet not connected to PC
3. WAN port	On	ATA network connection established
	Flashing	Data traffic on cable network
	Off	Waiting for network connection
4. FXS(Port1)	Off	Telephone Set is On-Hook
	Flashing	Ring Indication
	On	Telephone Set is Off-Hook
5. FXO(Port2)	Off	Line is On-hook
	On	Line is In-Use

065-9061 /065-9062

LED	State	Description
1. POWER	On	ATA is power ON
	Off	ATA is power Off
2. LAN port	On	LAN is connected successfully
	Flashing	Data is transmitting
	Off	Ethernet not connected to PC
3. WAN port	On	ATA network connection established
	Flashing	Data traffic on cable network
	Off	Waiting for network connection
4. Phone 2 (FXS 2)	Off	Telephone Set is On-Hook
	Flashing	Ring Indication
	On	Telephone Set is Off-Hook
5. Phone 1 (FXS 1)	Off	Telephone Set is On-Hook
	Flashing	Ring Indication
	On	Telephone Set is Off-Hook
6. WLAN port	On	Wireless network connection established
	Flashing	Data traffic on cable network
	Off	Waiting for network connection

1.7 ATA / Wi-Fi ATA Specification

VoIP Key Features:

- Support SIP protocols: SIP Registration and Digest Authentication.
- Smart VoIP call Dialing Book: VoIP call Book could provide any application VoIP call to any type destination (Domain name/IP address, PSTN or PBX) or hunting number setting.
- NAT traversal: This feature allows ATA to operate behind any NAT/Firewall device. There is no need to change any configuration of NAT/Firewall like setting virtual server.
- Smart-QoS Guaranteed: This bandwidth management feature provide good voice quality when user place VoIP call and access internet at the same time. The ATA will start reserve bandwidth for voice traffic automatically when VoIP call proceeds.
- Voice channels status display: This function display each port status like as On-hook, Off-hook, calling number callee's number, talk duration, codec.

Telephony Specification:

- Voice Codec: G.711(A-law /μ-law), G.729 AB, G.723 (6.3 Kbps / 5.3Kbps), G.276 (16,24,32,40 Kbps)
- FAX support : T.38,G.711 Fax pass-through
- G.168-2000 Line Echo Canceller.
- Call Waiting
- Call Hold/Resume
- Call Transfer: Blind Transfer / Early Attended Transfer / Attended Transfer
- Call Forward: On Busy Forward / No Condition forward / No Answer Forward
- Call Screen: Incoming Call Screen (Reject or Forward Incoming Call) / Outgoing Call Screen (Blocking Outgoing Call)
- Multi-Line Appearance
- DTMF Relay : In-band DTMF Relay / Out-of-band DTMF Relay (RFC2833)
- **3-Way Conference**

IP Specification:

- SIP (RFC 3261) , SDP (RFC 2327), Symmetric RTP,
- STUN (RFC3489), ENUM (RFC 2916), RTP Payload for DTMF Digits (RFC2833), Outbound Proxy Support, uPnP(UpnPTM)
- LAN :NAT, DHCP Server
- WAN: PPPoE client, DHCP client, Fix IP Address, DDNS client
- Network Address Translation: Providing build-in NAT router function.
- Static Routing
- Virtual Server
- Virtual DMZ
- QoS : IP TOS (IP Precedance) / DiffServ

Call Features:

- Voice channels CDR (Call Detail Record)
- Adjustable volume : - 9 db ~ 9 db
- VAD (Voice Activity Detection)
- Dynamic Jitter Buffer
- CNG (Comfort Noise Generation)
- Lost Packet Concealment
- Caller ID Detection: DTMF CID / Bellcore CID / ETSI CID /
- NTT CID Detection (Optional)
- Caller ID Generation: DTMF CID / Bellcore CID / ETSI CID /
- NTT CID Generation (Optional)

Configuration & Management:

- Web-based Graphical User Interface
- Remote management over the IP Network
- FTP firmware upgrade
- Backup and Restore Configuration file
- Auto Provisioning

General Specification:

- AC power : AC100V-240V, DC12V/1.5A,50/60 Hz
- Temperature: 0℃ ~ 40℃ (Operation)
- Humidity: up to 90% non-condensing
- Emission: FCC Part 15 Class B, CE Mark
- Dimension : 170 x 100 x 35 mm
- Weight: 200g

Wireless LAN:

- Standards : IEEE 802.11g / IEEE 802.11b / IEEE 802.11.(54Mbps)
- Wireless Frequency Range : 2.4GHz – 2.4835 GHz.
- Wireless Distribution System :Access point.
- Security :64/128 bit WEP data encryption ,WPA-PSK, WPA-EAP
- Wireless Signal Range : Indoors: Up to 280 ft (90 meters) / Outdoors: Up to 1180 ft (360 meters)
- Modulation Technology :802.11b: 11Mbps,5.5Mbps:CCK,2Mbps DQPSK,1Mbps DBPSK / 802.11g:54Mbps,48Mbps,36Mbps,24Mbps,18Mbps,12Mbps19Mbps,6Mbps OFDM.
- External Antenna Type : 2dBi Gain detachable dipole antenna with reverse SMA connector.

Installation and Setup

2.1 Package Content

Please check enclosed product and its accessories before installation. (Refer to the item number). These contents are from pre-released product. The contents for the final product might change a little bit.

065-9055/065-9056 Package

The ATA packet contents:

ATA(065-9055 / 065-9056 Series)	X1
RJ-45	X1
AC Power Adapter	X1
CD-Rom(User manual)	X1

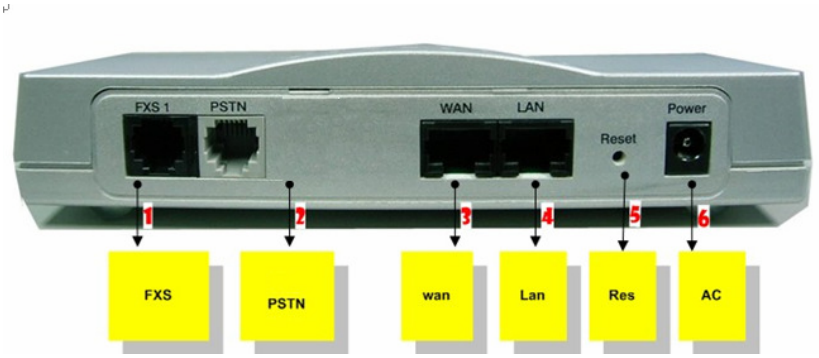
065-9061/065-9062 Package

The Wi-Fi ATA packet contents:

Wi-Fi ATA (065-9061 / 065-9062	X1
Series)	X1
RJ-45	X1
AC Power Adapter	X1
CD-Rom(User manual)	

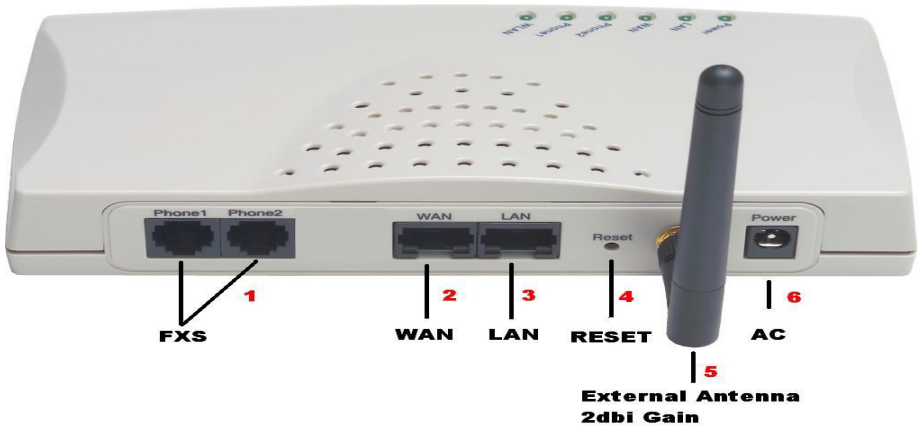
2.2Hardware Installation

Port Description: DEMO Model 065-9055



Item	Port	Description
1	FXS(Foreign Exchange Station)	FXS port can be connected to analog telephone sets or Trunk Line of PBX.
	PSTN	Can be Connected to PBX or CO line with RJ-11 analog line. PSTN not FXO port, can't connect PSTN to VoIP, It only FXS port extension. When PSTN call incoming , it will transfer to FXS port, let FXS can pick up call from VoIP or PSTN.
3	WAN(Wide Area Network)	Connect to the network with an Ethernet cable. This port allows your ATA to be connected to an Internet Access device, e.g. router, cable modem, ADSL modem, through a networking cable with RJ-45 connectors used on 10BaseT and 100BaseTX networks.
4	LAN(Local Area Network)	Connect to PC with Ethernet cable. 1 port allows your PC or Switch/Hub to be connected to the ATA through a networking cable with RJ-45 connectors used on 10BaseT and 100BaseTX networks.
5	RES(Reset button)	Push this button until 3 seconds, and ATA will be set to factory default configuration.
6	AC power(DC in 12V)	A power supply cable is inserted

Port Description: DEMO Model 065-9062



Item	Port	Description
1	FXS(Foreign Exchange Station)	FXS port can be connected to analog telephone sets or Trunk Line of PBX.
2	WAN(Wide Area Network)	Connect to the network with an Ethernet cable. This port allows your ATA to be connected to an Internet Access device, e.g. router, cable modem, ADSL modem, through a networking cable with RJ-45 connectors used on 10BaseT and 100BaseTX networks.
3	LAN(Local Area Network)	Connect to PC with Ethernet cable. 1 port allows your PC or Switch/Hub to be connected to the ATA through a networking cable with RJ-45 connectors used on 10BaseT and 100BaseTX networks.
4	RES(Reset button)	Push this button until 3 seconds, and ATA will be set to factory default configuration.
5	External Antenna 2db Gain (Wireless LAN Area Network).	Used to Wirelessly Connect to 802.11b/g networks. 802.11b: 11Mbps,5.5Mbps:CCK,2Mbps DQPSK,1Mbps DBPSK .802.11g:54Mbps,48Mbps,36Mbps,24Mbps,18Mbps,12Mbps19Mbps,6Mbps OFDM.
6	AC power(DC in 12V)	A power supply cable is inserted

Installation:

1 Connect the 12V DC IN to the power outlet with power adaptor.
2 Connect FXO to PSTN.
3 Connect FXS to a telephone jack with the RJ-11 analog cable.

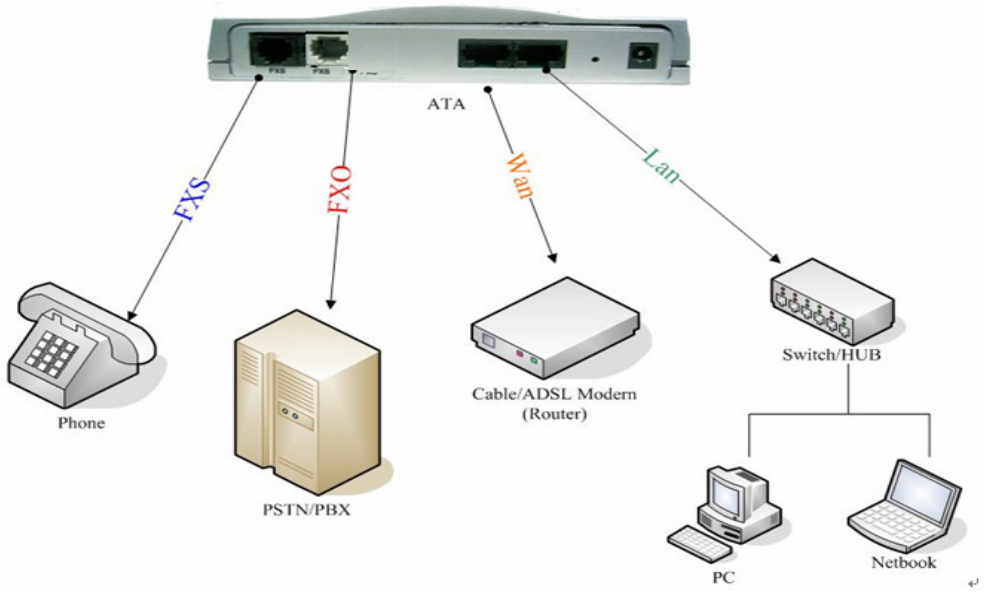
Connecting to a PC:

1 Connect the Ethernet cable (with RJ-45 connector) to any LAN port.
2 Connect the other end of the Ethernet cable to your PC's installed network interface card (NIC).

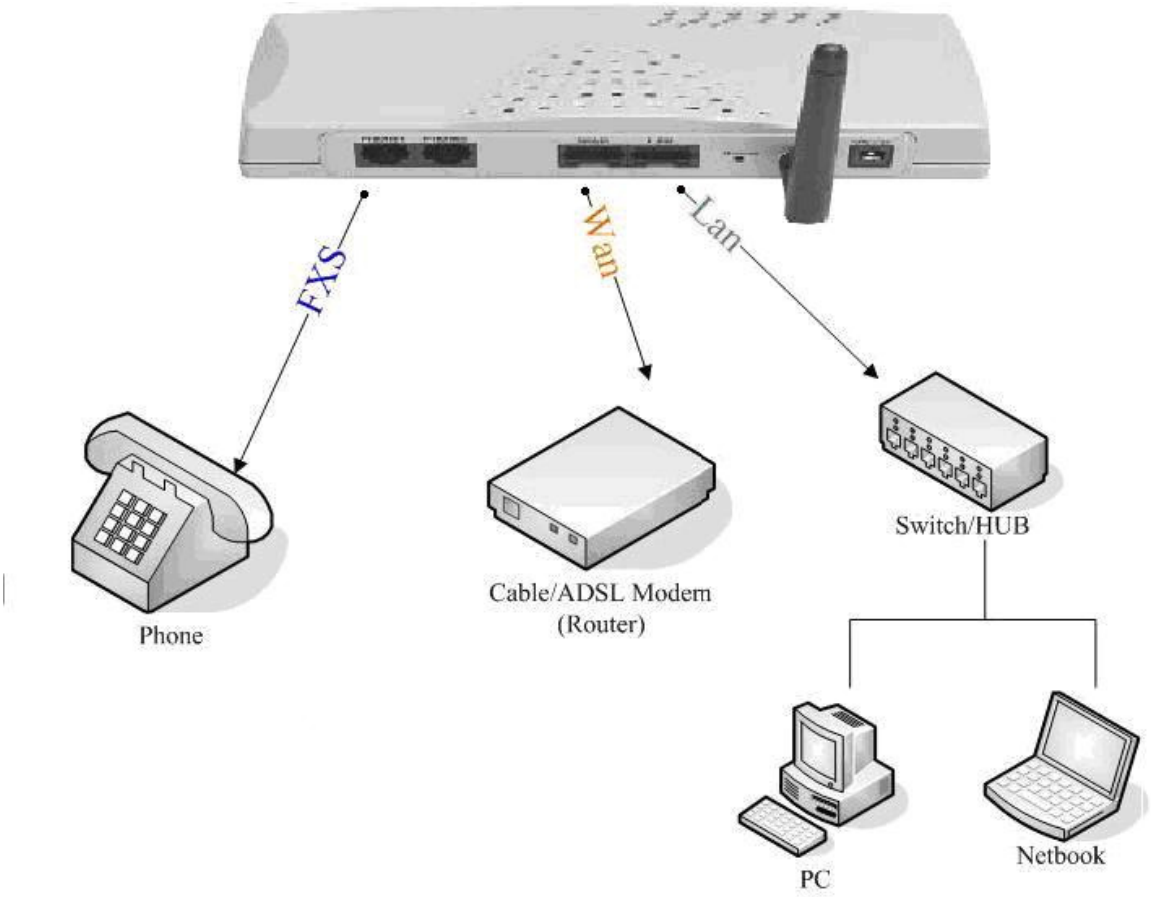
Connecting to an External Ethernet Hub or Switch:

1 Connect the Ethernet cable (with RJ-45 connector) to WAN port.
2. Connect the other end of the Ethernet cable to DSL/Cable modem or the external Ethernet hub or switch.

065-9055/065-9056



065-9062/065-9061



2.3Quick Start

How to set your network environment?

ATA default network environment:
For Wan:
IP: 192.168.1.1
Subnet mask: 255.255.0.0
Default Gateway: 192.168.1.254
For Lan:
IP: 222.222.222.1
Subnet mask: 255.255.0.0
Default Gateway: 222.222.222.254

How to configure ATA?

1. Configure your PC or NB to the same subnet with ATA.
2. Use web browser (IE/Firefox) link to url: http://192.168.1.1:8888 (If you connect to LAN port, link to url: http://222.222.222.1)
3. Login user name: admin
4. Login password: admin
5. Use this web configuration interface to configure all system functionality; firstly you should change the WAN network environment to yours.

How to use VoIP?

1. Configure SIP user account to register your SIP proxy, use web configuration:
   "SIP Settings" -> "Account Setting"
   a. Port Phone Number
   b. Port Authentication User Name
   c. Port Authentication Password
   d. Confirmed Password
2. Configure SIP registrar server and proxy server, use web configuration:
   "SIP Settings" -> "Server Setting"
   a. Registrar Server Address
   b. Outbound Proxy Address
3. Make sure ATA has already registered to your proxy, and then you can make a call

How to make a three way conference call?

1. Make a call to the first party.
2. "Flash hook" to hold the call.
3. Dial "**", and then you will hear a dial tone.
4. Make the other call to the third party.
5. Dial "*3" to connect the two party calls for conferencing.

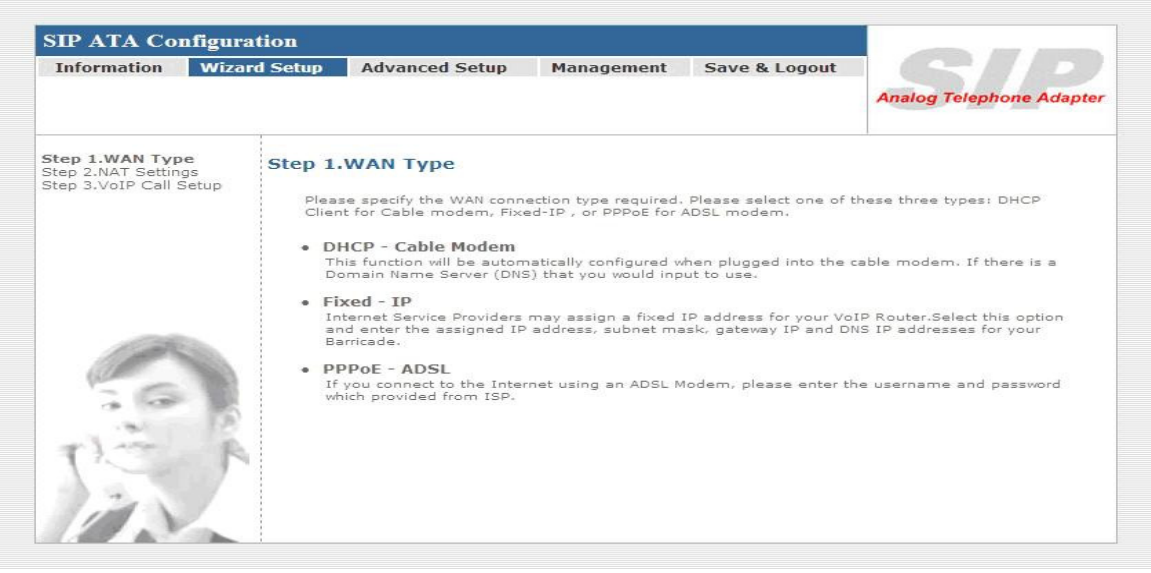
2.4 Wizard Setup

Wizard for Quick Setup ATA, after finishing the authentication, the Main menu will display 5 parts of configuration, please click "Wizard Setup" to enter quick start:

WAN Port Type Setup:

For most users, Internet access is the primary application. The **SA** Series ATA support the WAN interface for Internet access and remote access. The following sections will explain more details of WAN Port Internet access and broadband access setup. When you click "**WAN Port Type Setup**" from within the Wizard **Setup**, the following setup page will be show.

Three methods are available for Internet Access:

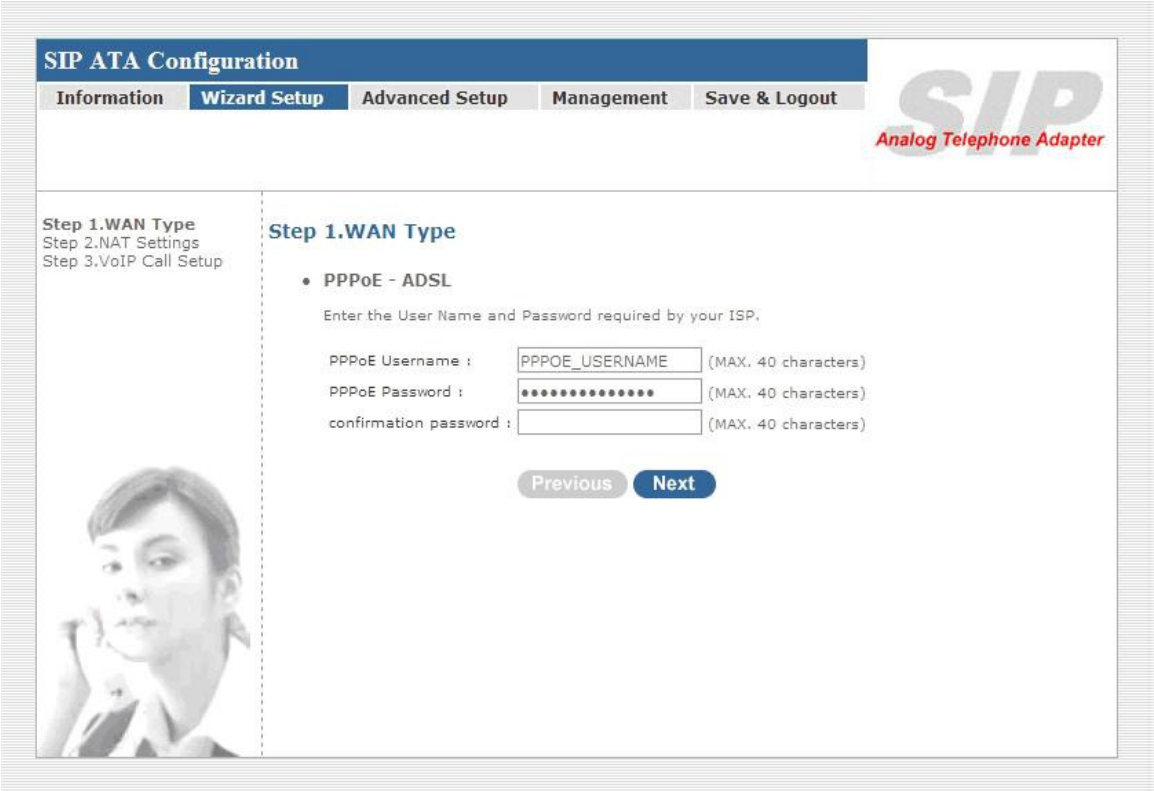

SIP ATA Configuration
Information
Wizard Setup
Advanced Setup
Management
Save & Logout
SIP
Analog Telephone Adapter
Step 1.WAN Type
Step 2.NAT Settings
Step 3.VoIP Call Setup
Step 1.WAN Type
Please specify the WAN connection type required. Please select one of these three types: DHCP Client for Cable modem, Fixed-IP , or PPPoE for ADSL modem.
DHCP - Cable Modem
This function will be automatically configured when plugged into the cable modem. If there is a Domain Name Server (DNS) that you would input to use.
Fixed - IP
Internet Service Providers may assign a fixed IP address for your VoIP Router.Select this option and enter the assigned IP address, subnet mask, gateway IP and DNS IP addresses for your Barricade.
PPPoE - ADSL
If you connect to the Internet using an ADSL Modem, please enter the username and password which provided from ISP.

Fixed IP User: If you are a leased line user with a fixed IP address, fill out the following items with the information provided by your ISP.

- **WAN IP Address:** check with your ISP provider
- **Subnet mask:** check with your ISP provider
- **Default Gateway:** check with your ISP provider

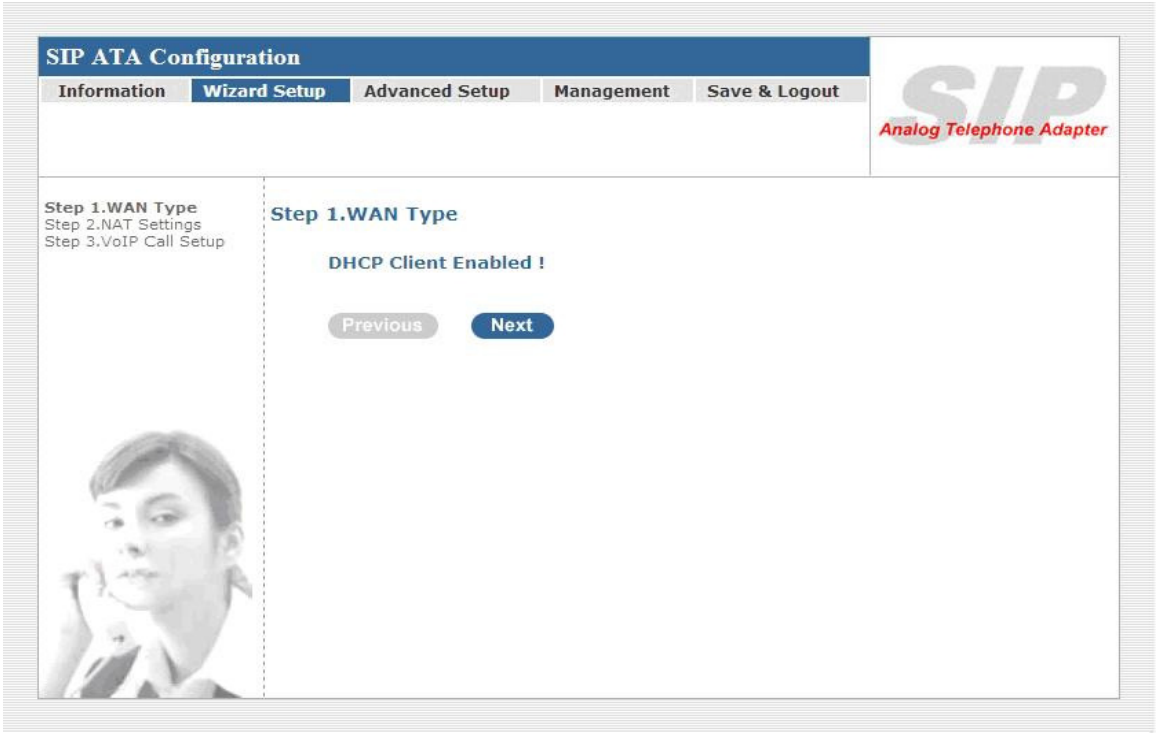
ADSL Dial-Up User (PPPoE Enable)

Some ISPs provide DSL-based service and use PPPoE to establish communication link with end-users. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you need to select this item.



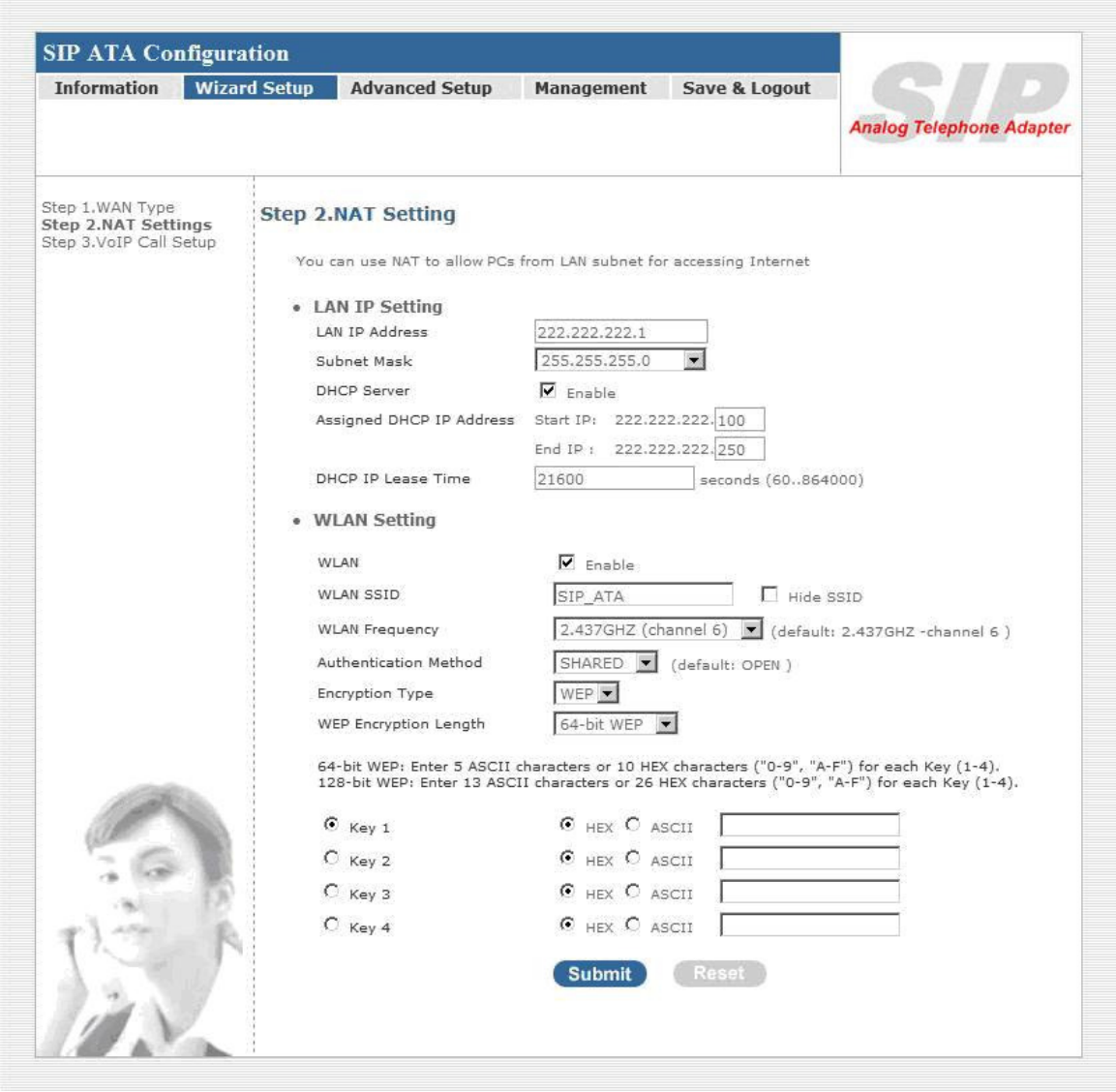
- **PPPoE User Name:** Enter User Name provided by your ISP
- **PPPoE Password:** Enter Password provided by your ISP.
- **Confirmation Password:** Enter Password to confirm again.

DHCP Client (Dynamic IP): Get WAN IP Address automatically



- **IP Address:** If you are connected to the Internet through a Cable modem line then a dynamic IP address will be assigned.

NAT setting:


SIP ATA Configuration
Information
Wizard Setup
Advanced Setup
Management
Save & Logout
SIP
Analog Telephone Adapter
Step 1.WAN Type
Step 2.NAT Settings
Step 3.VoIP Call Setup
Step 2.NAT Setting
You can use NAT to allow PCs from LAN subnet for accessing Internet
LAN IP Setting
LAN IP Address 222.222.222.1
Subnet Mask 255.255.255.0
DHCP Server Enable
Assigned DHCP IP Address Start IP: 222.222.222.100
End IP : 222.222.222.250
DHCP IP Lease Time 21600 seconds (60..864000)
WLAN Setting
WLAN Enable
WLAN SSID SIP_ATA Hide SSID
WLAN Frequency 2.437GHZ (channel 6) (default: 2.437GHZ -channel 6)
Authentication Method SHARED (default: OPEN)
Encryption Type WEP
WEP Encryption Length 64-bit WEP
64-bit WEP: Enter 5 ASCII characters or 10 HEX characters ("0-9", "A-F") for each Key (1-4).
128-bit WEP: Enter 13 ASCII characters or 26 HEX characters ("0-9", "A-F") for each Key (1-4).
Key 1 HEX ASCII
Key 2 HEX ASCII
Key 3 HEX ASCII
Key 4 HEX ASCII
Submit
Reset

- **LAN IP Address:** Private IP address for connecting to a local private network (Default: 222.222.222.1).
- **Subnet Mask:** Subnet mask for the local private network (Default: 255.255.255.0).
- **DHCP Server:** Enable to open Lan port DHCP server, disable is bridge mode.
- **Assigned DHCP IP Address:** DHCP server range from start IP to end IP.
- **DHCP IP Lease Time:** Client to ask DHCP server refresh time**,** range from 60 to 86400 seconds.

065-9062/065-9061 Only

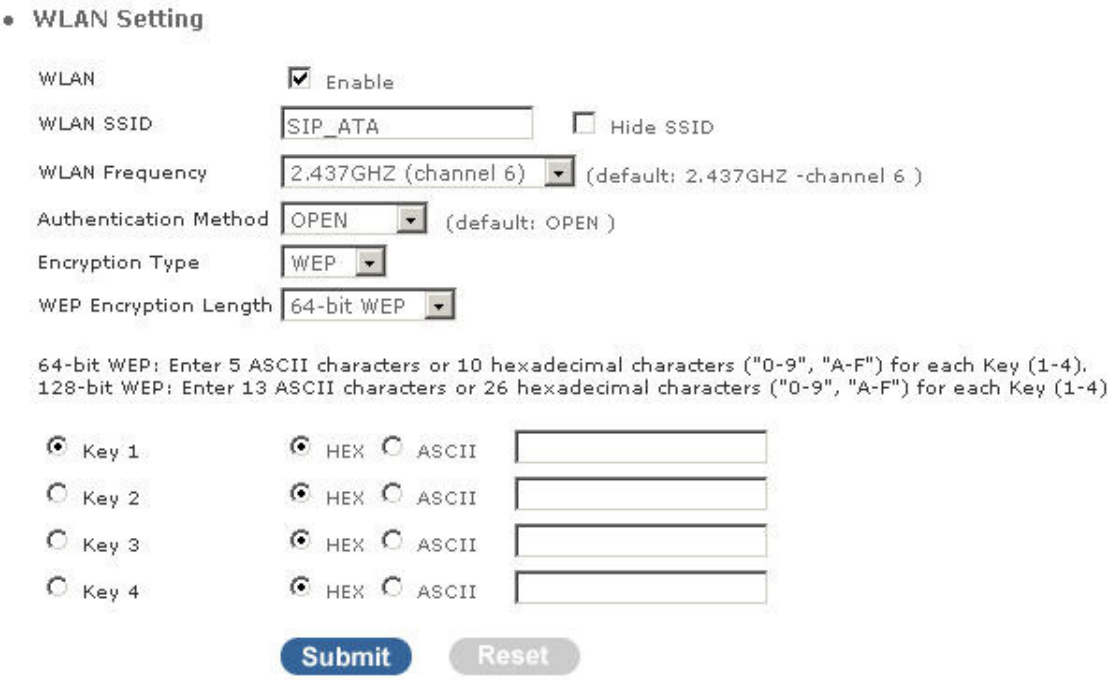
- **WLAN:** Enable/Disable Wireless function.(Access Point)
- **WLAN SSID:** The service set Identifier assigned to the wireless network(WLAN).Default SSSI is SIP_ATA.
- **WLAN Frequency:** Set the operating frequency/channel depending on your particular region.(Default frequency is 2.437Ghz.)
- **Authentication Method:** OPEN,SHARED,WPA-EAP,WPA-PSK Mode .Default is OPEN.
- **Encryption type:** None or WEP(Enable WEP Encryption mode)
- **WEP Encryption Lenuth:** Select 64-bit WEP or 128 bit WEP to Enable data encryption
- **Key 1- Key 4 (HEX / ACSII):** The WEP keys are used to encrypt data. Both the Prestige And the wireless stations,must use the same WEP key for data transmission.(Default Key is Key 1).

64-bit WEP ; 5 ACSII Characters / 10 hexadecimal characters (“0 - 9”, “A - F).
128-bit WEP ; 13 ACSII Characters / 26 hexadecimal characters (“0 - 9”, “A - F).

WLAN Setting

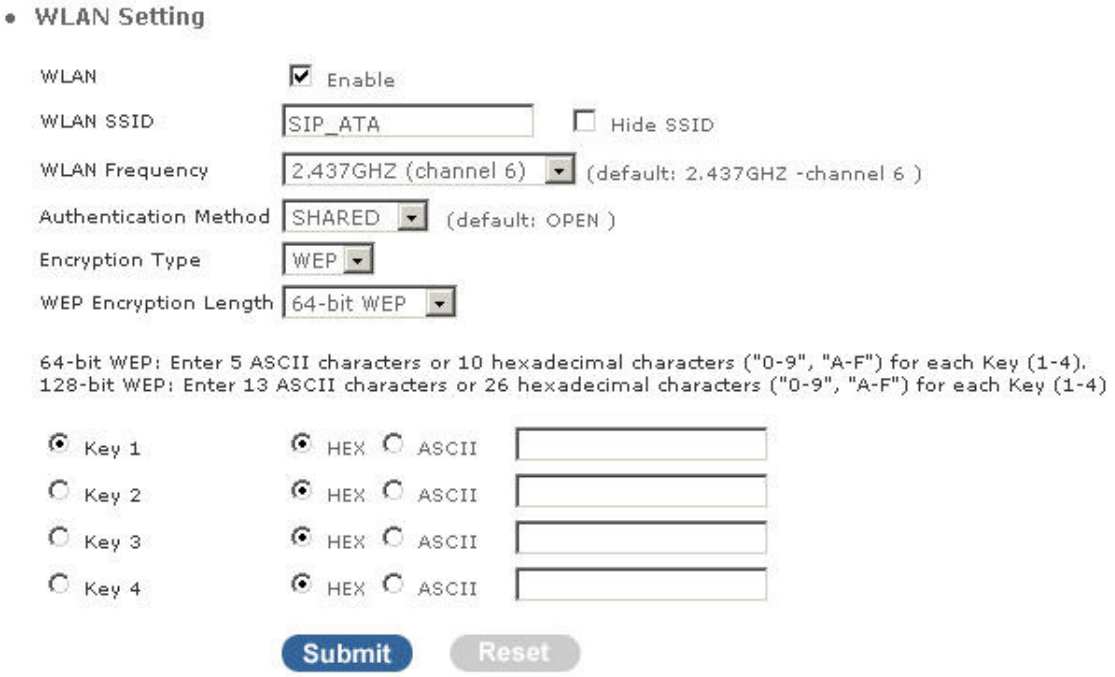
Authentication Method:

OPEN Mode (WEP)



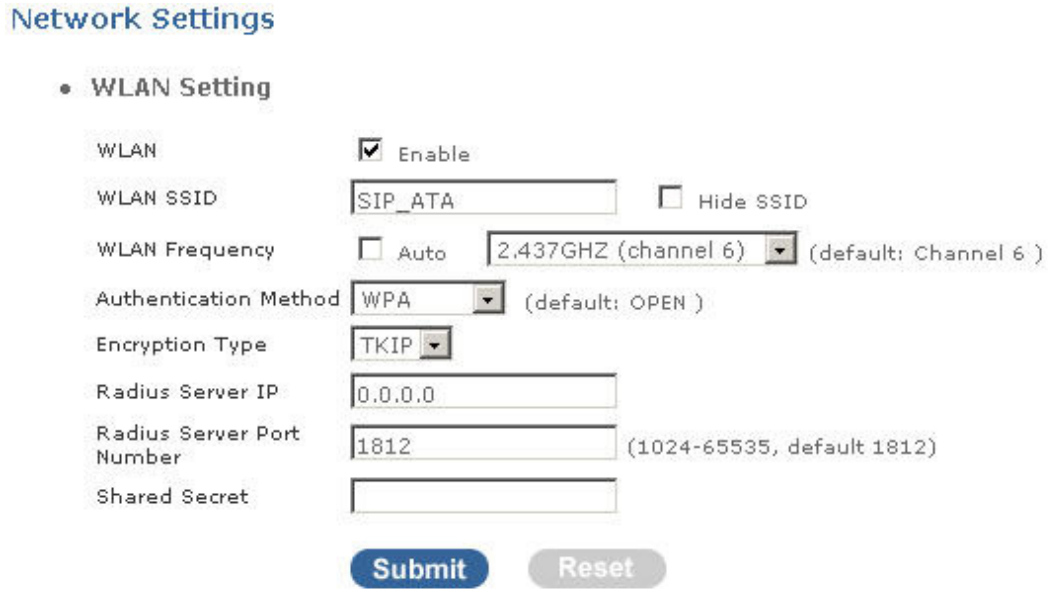
Encryption Type : Select None or WEP.(default is NONE Type).
WEP Encryption Length : Select 64-bit WEP or 128-Bit WEP.
WEP Key : Select Key 1 or Key 2 ,Key 3 , Key 4. to be the active key.
WEP Key Type : HEX or ACSII. (HEX Characters : 0-9 ,A-F. ASCII Characters : 0-9 ,A-Z.)

SHARED Mode (WEP)



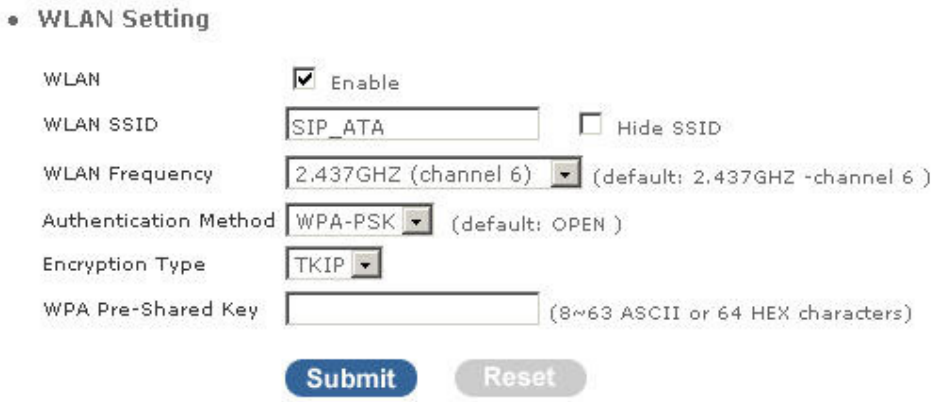
Encryption Type : WEP
WEP Encryption Length : Select 64-bit WEP or 128-Bit WEP.
WEP Key : Select Key 1 or Key 2 ,Key 3 , Key 4. to be the active key.
WEP Key Type : HEX or ACSII. (HEX Characters : 0-9 ,A-F. ASCII Characters : 0-9 ,A-Z.)

WPA-EPA Mode (Need Radius Server)



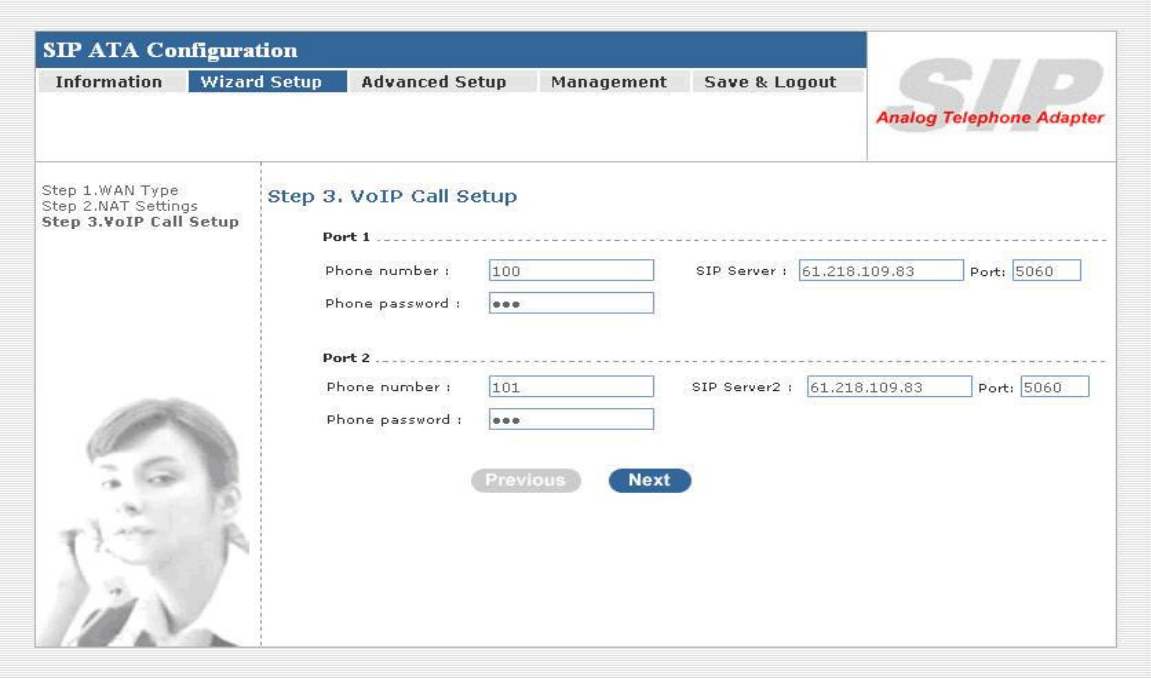
IP Address : Radius Server IP.
Port Number :Radius Server Port.
Shared Secret “Radius Secret.

WPA-PSK Mode



Encryption Type :TKIP or AES mode.
WEP Encryption Length : Select 64-bit WEP or 128-Bit WEP.
WEP Key : Select Key 1 or Key 2 ,Key 3 , Key 4. to be the active key.
WEP Key Type : HEX or ACSII.(8 to 63 ACSII or 64 HEX Characters).

VoIP Call Setup



Step 1 : configure the numbering with phone/line ports.

- **Phone Number (FXS):** The representation number is the phone number of the telephone that is connected to Phone port.
- **Line Number (FXO):** Line ports are connected to the extension ports of the PBX system or the PSTN line. They have a common Line Hunting Group Number. When this number is dialed, the ATA will find a free FXO line connected to PBX. This hunting will skip all busy lines and absent lines and find only the idle line to the PBX. After the available line is found, you can hear the dial tone from PBX. After that, you can dial the needed phone number out through PBX.

Step 2: Let ATA Register to SIP Proxy Server

- **SIP Proxy Server IP addresses:** There is a SIP Proxy Server address and port fields. Check with your ITSP provider.
- **Phone number** / **password:** check with your ISP provider.

Step 3: Finishing the Wizard Setup

After completing the Wizard Setup, please click “Finish” bottom. The ATA will save the configuration and rebooting ATA automatically. After 20 Seconds, you could re-login the ATA.

Network Setting

- WAN Setting
- LAN Setting
- DHCP Setting
- Static Route (Default Router)
- NAT
- Packet Filter
- URL Filter
- Security
- UPNP
- DDNS

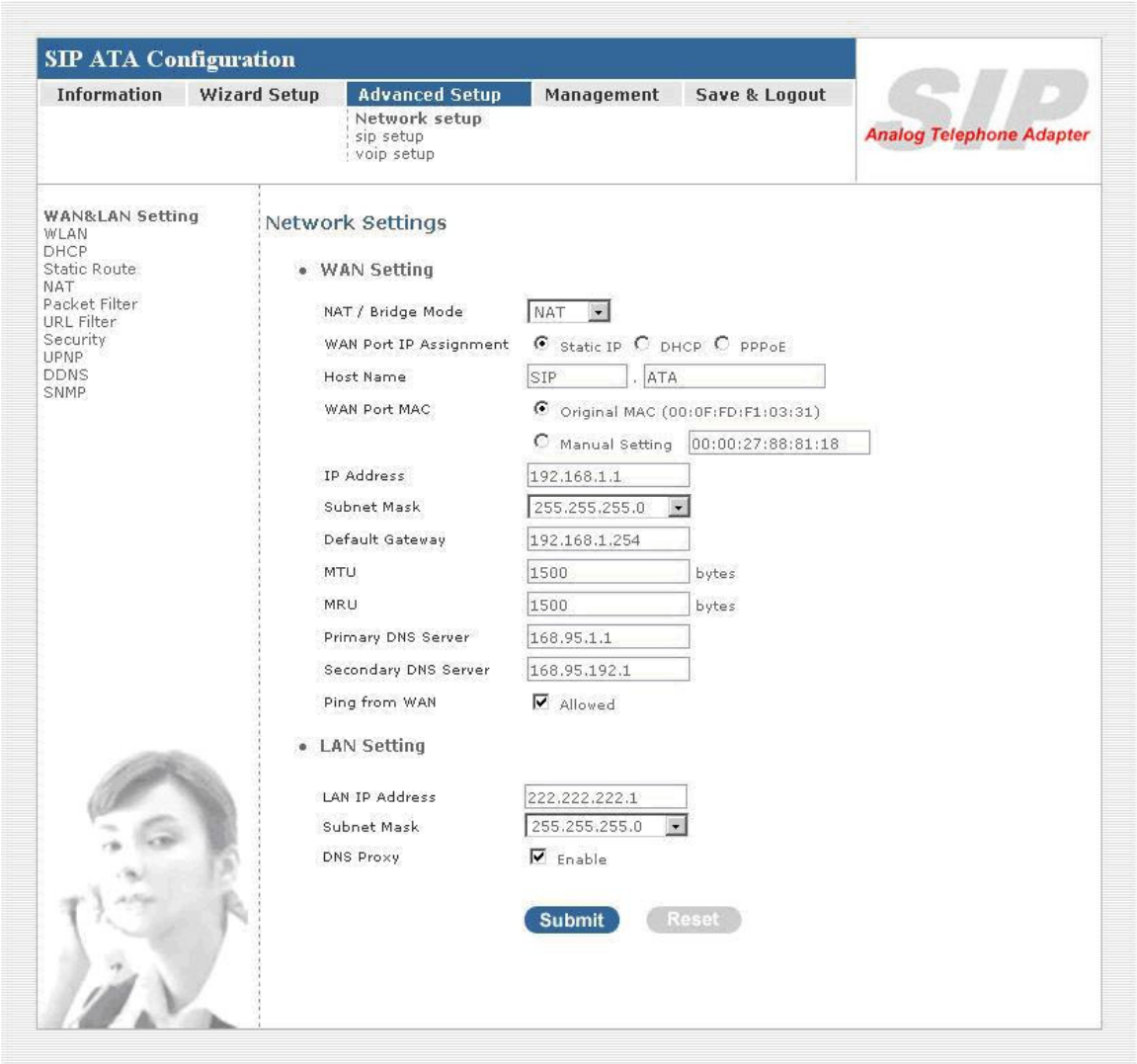
3.1 WAN Setting

WAN (Wide Area Network) is a network connection connecting one or more LANs together over some distance. For example, the means of connecting two office buildings separated by several kilometers would be referred to as a WAN connection. The size of a WAN and the number of distinct LANs connected to a WAN is not limited by any definition. Therefore, the Internet may be called a WAN.

WAN Settings are settings that are used to connect to your ISP (Internet Service Provider). The WAN settings are provided to you by your ISP and often times referred to as "public settings". Please select the appropriate option for your specific ISP.

For most users, Internet access is the primary application. ATA supports the WAN interface for internet access and remote access. The following sections will explain more details of WAN Port Internet access and broadband access setup. When you click “WAN Setting”, the following setup page will be shown. Three methods are available for Internet Access.

- Static IP
- DHCP
- PPPoE

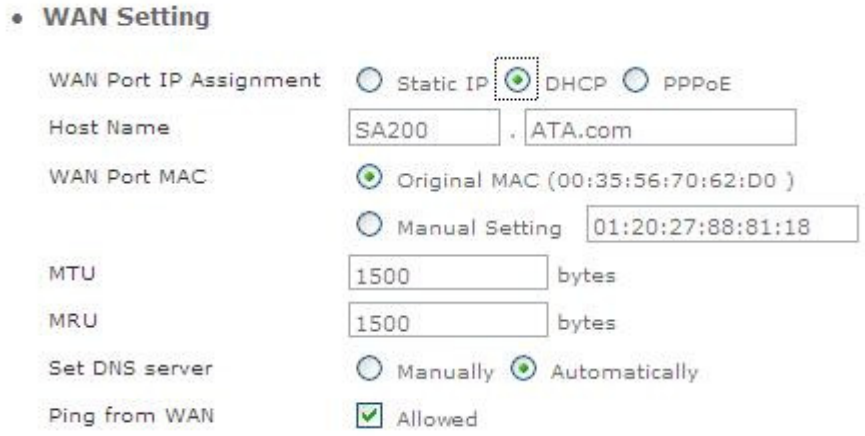


Static IP

If you are a leased line user with a fixed IP address, enter in the IP address, subnet mask, gateway address, and DNS (domain name server) address(es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.
Example: 168.95.1.2
■IP Address: Check with your ISP provider.
■Subnet Mask: Check with your ISP provider.
■Default Gateway: Check with your ISP provider.

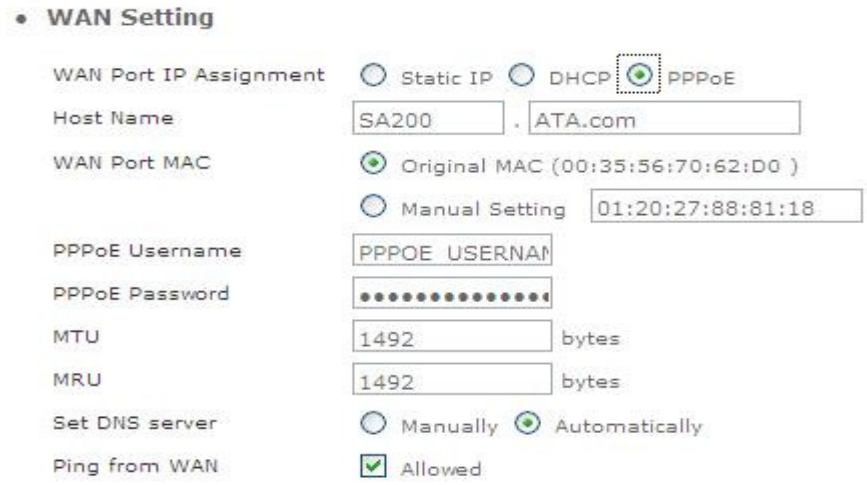
DHCP

Dynamic Host Configuration Protocol (DHCP), Dynamic IP (Get WAN IP Address automatically). If you are connected to the Internet through a Cable modem line, then a dynamic IP will be assigned.
Note: WAN port gets the IP Address, Subnet Mask and default gateway IP address automatically, if DHCP client is successful.



PPPoE

Point-to-Point Protocol over Ethernet (PPPoE). Some ISPs provide DSL-based services and use PPPoE to establish communication link with end-users. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you need to make sure the following items, PPPoE User name: Enter username provided by your ISP. PPPoE Password: Enter password provided by your ISP.



Host Name

The Host Name field is optional but may be required by some Internet Service Providers. The default host name is the model number of the device. It is a computer that is connected to a TCP/IP network, including the Internet. Each host has a unique IP address. Assign the domain name or IP address of your host computer. When the host operating system is set up it is given a name. This name may reflect the prime use of the computer. For example, a host computer that converts host names to IP addresses using DNS may be called cvs.ata.com and a host computer that is a web server may be called www.ata.com. When we need to find the host name from an IP address we send a request to the host using its IP address. The host will respond with its host name.

WAN Port MAC

The MAC (Media Access Control) Address field is required by some Internet Service Providers (ISP). The default MAC address is set to the MAC address of the WAN interface in the device. It is only necessary to fill the field if required by your ISP.

The WAN port allows your voice gateway to be connected to an Internet Access Device, e.g. router, cable modem, ADSL modem, through a CAT.5 twisted pair Ethernet Cable.

MAC addresses are uniquely set by the network adapter manufacturer and are sometimes called "physical addresses" for this reason. MAC assigns a unique number to each IP network adapter called the MAC address. The MAC address is commonly written as a sequence of 12 hexadecimal digits as follows:00:0f:fd: 88:81:18 The first six hexadecimal digits of the address correspond to a manufacturer's unique identifier, while the last six digits correspond to the device's serial number.

Some Internet service providers track the MAC address of a home router for security purposes. Many routers support a process called cloning that allows the MAC address to be simulated so that it matches one the service provider is expecting. This allows end-user to change their router (and their real MAC address) without having to notify the provider.

For example, you could allow packets which have your name server's IP on them, but come from another MAC address (one way of spoofing packets).

MTU and MRU

MTU stands for Maximum Transmission Unit, the largest physical packet size, measured in bytes that a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent.

MRU stands for Maximum Receiving Unit. The largest physical packet size, measured in bytes that a network can receive. Any messages larger than the MRU are divided into smaller packets before being received.

The key is to be deciding how big your bandwidth pipe is and select the best MTU for your configuration. For example, you have a 33.6 modem, you use a MTU and MRU of 576, and if you have a larger pipe you may want to try 1500.

For Static IP, both MTU and MRU are set to 1500 bytes as default value.
For DHCP, both MTU and MRU are set to 1500 bytes as default value.
For PPPoE, both MTU and MRU are set to 1492 bytes as default value.

DNS Server

DNS stands for Domain Name System. Every Internet host must have a unique IP address; also they may have a user-friendly, easy to remember name such as www.ata.com The DNS server converts the user-friendly name into its equivalent IP address.

The original DNS specifications require that each domain name is served by at least 2 DNS servers for redundancy. When you run your DNS, web, and mail servers all on the same machine - if this machine goes down, it doesn't really matter that the backup DNS server still works.

The recommended practice is to configure the primary and secondary DNS servers on separate machines, on separate Internet connections, and in separate geographic locations.

□Primary DNS Server: Sets the IP address of the primary DNS server.
□Secondary DNS Server: Sets the IP address of the secondary DNS server.

Ping From WAN

Ping is a basic Internet program that lets you verify that a particular IP address exists and can accept requests. Ping is used diagnostically to ensure that a host computer you are trying to reach is actually operating.

The default setting is allowed user can ping the host computer from remote site. If you disallow, the host computer doesn't response any user who issues Ping IP address command from any remote sites.

3.2 LAN Setting

These are the IP settings of the LAN (Local Area Network) interface for the device. These settings may be referred to as "private settings". You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet. The default IP address is 222.222.222.1 with a subnet mask of 255.255.255.0.

LAN is a network of computers or other devices that are in relatively close range of each other. For example, devices in a home or office building would be considered part of a local area network.

□LAN IP Address: Assign the IP address of LAN server, default is 222.222.222.1

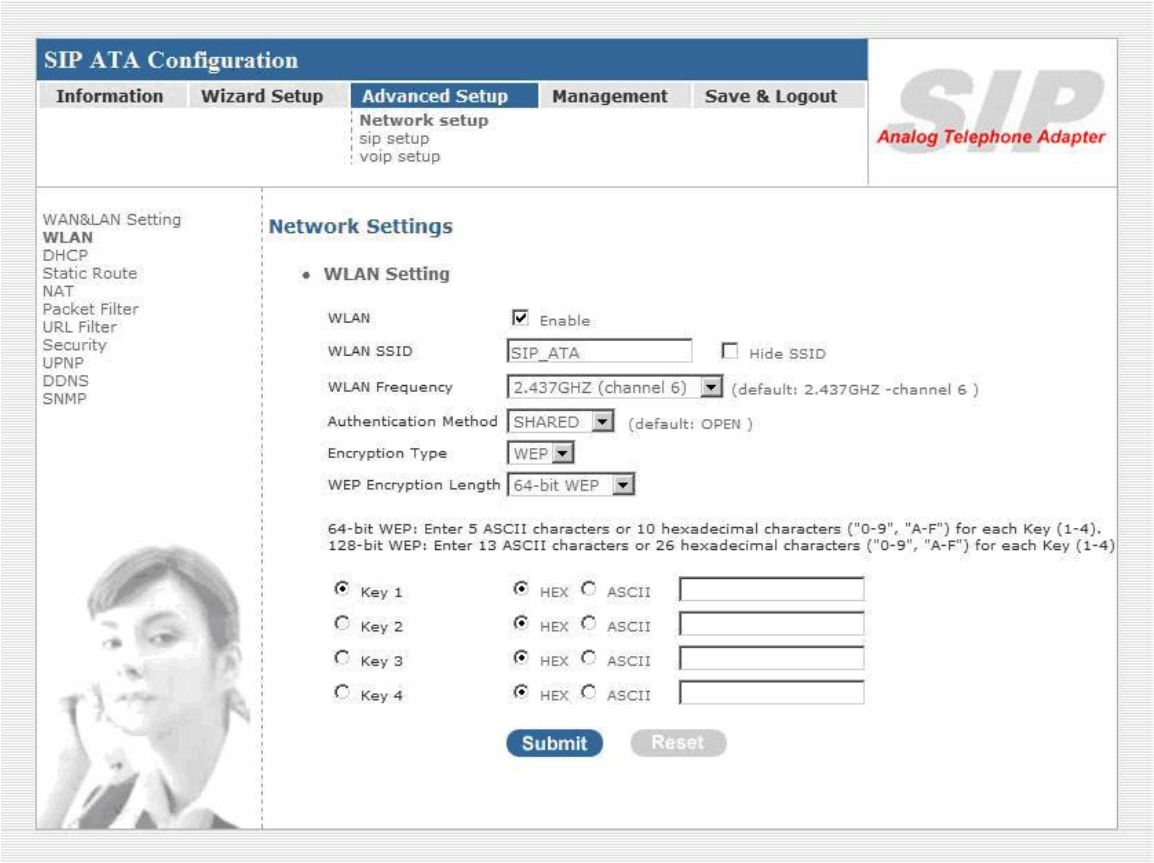
□Subnet Mask: Select a subnet mask from the pull-down menu, default is 255.255.255.0.

DNS Proxy

A proxy server is a computer network service that allows clients to make indirect network connections to other network services. The default setting is Enable the DNS proxy server.

3.3 WLAN Setting (Only 065-9061/065-9062 Model)

A WLAN is a data communication system that reduces the need for a wired connection, thereby adding new flexibility and convenience to your network. Using electromagnetic waves, WLAN's transmits and receives data over the air, minimizing the need for wired connections and combines data connectivity with user mobility. With a small investment, you can enjoy the same advantages of a wireless LAN; high data rates, security, standards compliance, compact size and extraordinary value.



□WLAN – Enable / Disable WLAN Function.(default is uncheck)
□WLAN SSID –The SSID "Service Set ID entity " identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point must have the same SSID. Enter a descriptive name for the wireless LAN.(support 20 ACSII characters)
□Hide SSID – Hide SSID prevents outside users from joining the network without knowing the wireless Network's ID ,default is check SSID.
□WLAN Frequency –The range of radio frequencies used by IEEE 802.11b/g wireless devices is called a Selection channel. Select a channel ID that is not already in use by a neighboring device.
□Authentication Method – Select Open,Shared,WPA,WPA-PSK.

	ENCRYPTION MOTHOD	ENTER Security KEY	IEEE 802.x b/g
OPEN	NONE	NO	NO
OPEN	WEP	NO	Enable with WEP key
		YES	Enable without WEP key
		YES	Disable
SHARED	WEP	NO	Enable with WEP key
		YES	Enable without WEP key
		YES	Disable
WPA-EAP	WEP	NO	YES
WPA-PSK	TKIP	YES	YES
WPA-PSK	AES	YES	YES

□Encryption Type – WEP / NONE.
□WEP Encryption lenugth –Select 64-bit WEP or 128 bit WEP to Enable data encryption
Key 1- Key 4 (HEX / ACSII): The WEP keys are used to encrypt data. Both the Prestige And the wireless stations,must use the same WEP key for data transmission.(Default Key is Key 1).
64-bit WEP ; 5 ACSII Characters / 10 hexadecimal characters (“0 - 9”, “A - F).
128-bit WEP ; 13 ACSII Characters / 26 hexadecimal characters (“0 - 9”, “A - F).

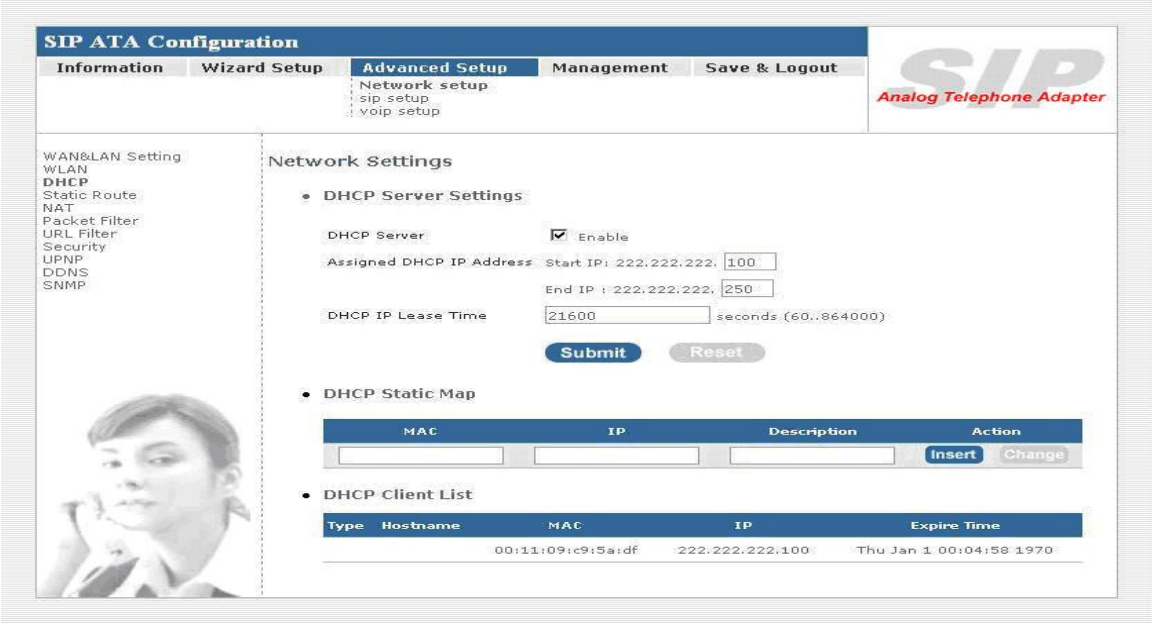
3.4 DHCP Server Setting

DHCP stands for Dynamic Host Control Protocol. The DHCP server gives out IP addresses when a device is starting up and request an IP address to be logged on to the network. The device must be set as a DHCP client to "Obtain the IP address automatically". By default, the DHCP Server is enabled in the unit. The DHCP address pool contains the range of the IP address that will automatically be assigned to the clients on the network.

DHCP client computers connected to the unit will have their information displayed in the DHCP Client List table. The table will show the Type, Host Name, IP Address, MAC Address, Description, and Expired Time of the DHCP lease for each client computer.

DHCP Server is a useful tool that automates the assignment of IP addresses to numbers of computers in your network. The server maintains a pool of IP addresses that you use to create scopes. (A DHCP scope is a collection of IP addresses and TCP/IP configuration parameters that are available for DHCP clients to lease.) Then, the server automatically allocates these IP addresses and related TCP/IP configuration settings to DHCP-enabled clients in the network. The DHCP Server leases the IP addresses to clients for a period that you specify when you create a scope. A lease becomes inactive when it expires. Through the DHCP Server, you can reserve specific IP addresses permanently for hardware devices that must have a static IP address (e.g., a DNS Server).

An advantage of using DHCP is that the service assigns addresses dynamically. The DHCP Server returns addresses that are no longer in use to the IP addresses pool so that the server can reallocate them to other machines in the network. If you disable this DHCP, you would have to manually configure IP for new computers, keep track of IP addresses so that you could reassign addresses that clients aren't using, and reconfigure computers that you move from one subnet to another. The DHCP Static MAP table lists all MAC and IP address which are active now.

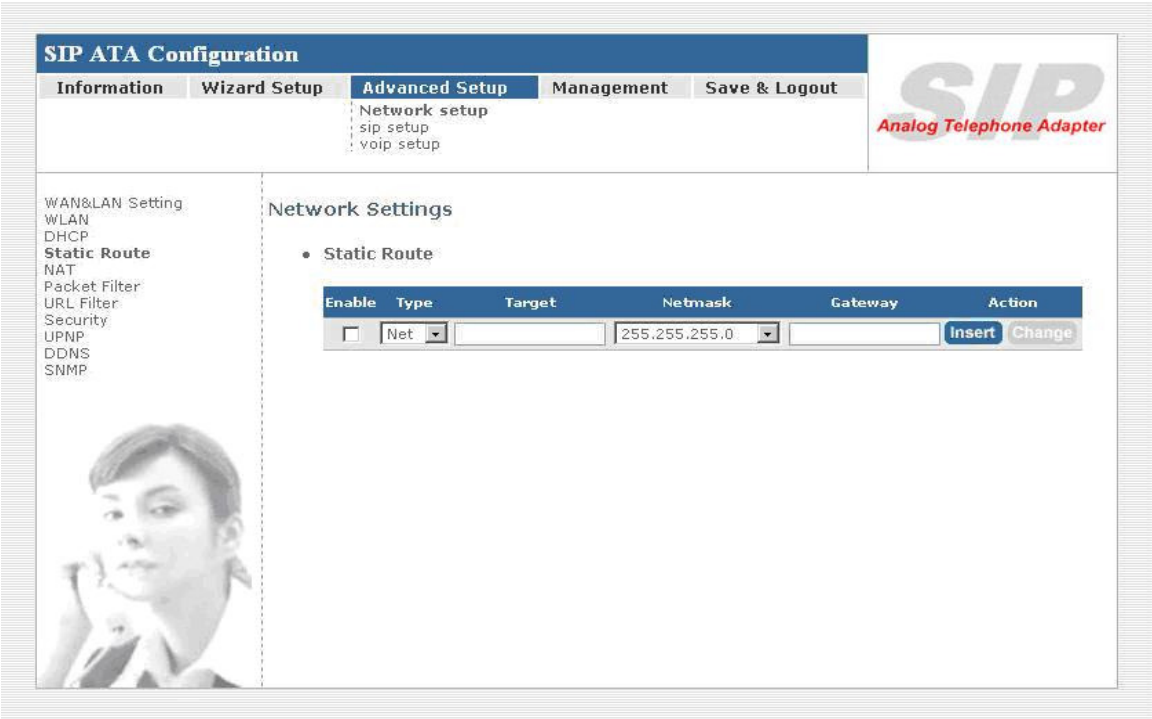


When you enable the DHCP server,
□Assigned DHCP IP Address: Enter the starting IP address for the DHCP server's IP assignment and the ending IP address for the DHCP server's IP assignment.
□DHCP IP Lease Time - Assign the length of time for the IP lease, default setting is 86400 seconds.

3.5 Static Router

Static routes are special routes that the network administrator manually enters into the router configuration. You could build an entire network based on static routes. The problem with doing this is that when a network failure occurs, the static route will not change without you performing the change. This isn't a good thing if the failure occurs during the middle of the night, or while you are on vacation.

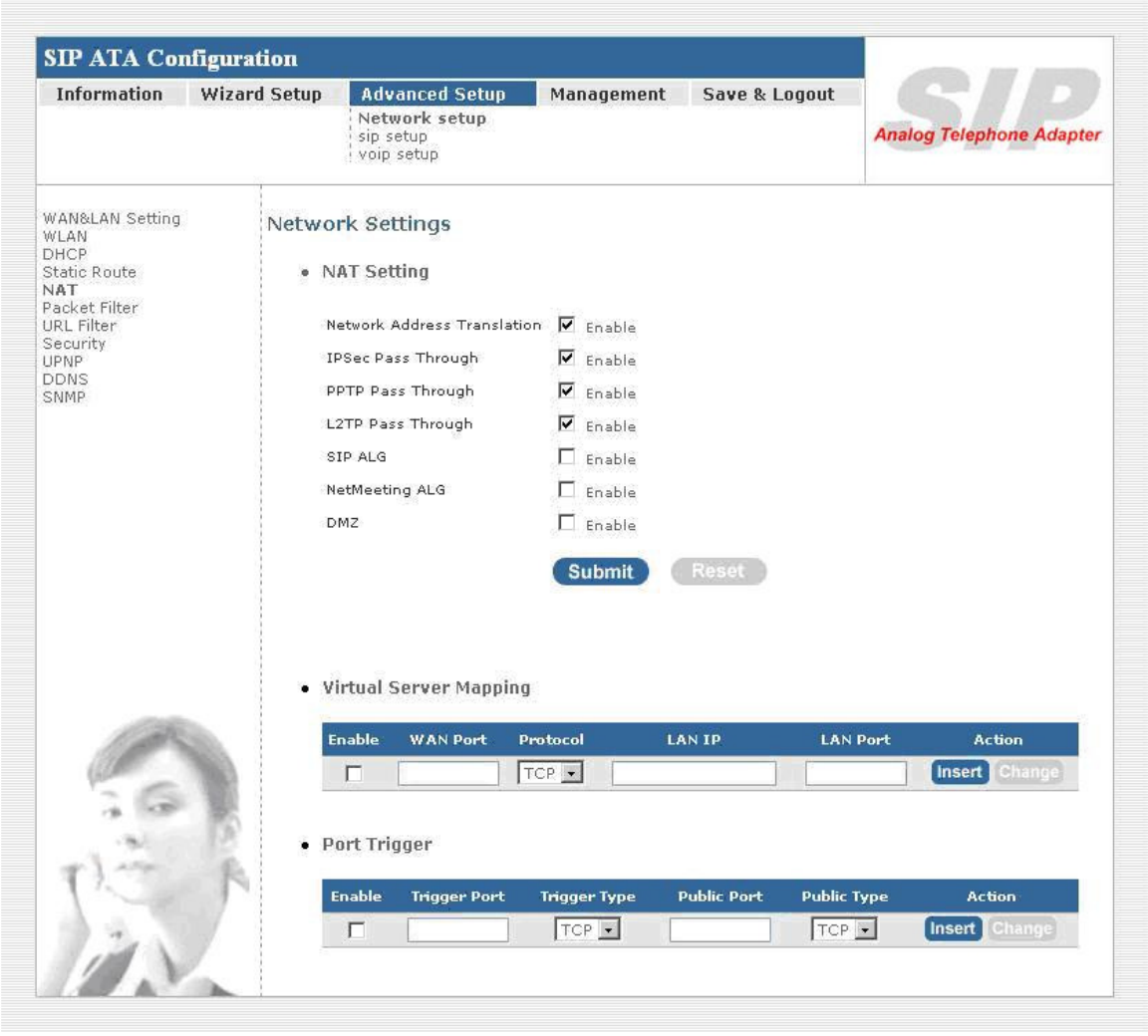
The route table allows the user to configure and define all the static routes supported by the router.



□Enable - Enable/Disable the static route.
□Type - Indicates the type of route as follows, Host for local connection and Net for network connection.
□Target - Defines the base IP address (Network Number) that will be compared with the destination IP address (after an AND with NetMask) to see if this is the target route.
□NetMask - The subnet mask that will be AND'd with the destination IP address and then compared with the Target to see if this is the target route.
□Gateway - The IP address of the next hop router that will be used to route traffic for this route. If this route is local (defines the locally connected hosts and Type = Host) then this IP address MUST be the IP address of the router
□Action - Insert a new Static Router entry or update a specified entry

3.6 NAT

NAT (Network Address Translation) serves three purposes:
1. Provides security by hiding internal IP addresses. Acts like firewall.
2. Enables a company to access internal IP addresses. Internal IP addresses that are only available within the company will not conflict with public IP.
3. Allows a company to combine multiple ISDN connections into a single internet connection.



NAT Setting

Network Address Translation - Enable/Disable NAT.
□IPSec Pass Through - IPsec (Internet Protocol Security) is a framework for a set of protocols for security at the network or packet processing layer of network communication. Enable/Disable this framework verification.

□PPTP Pass Through - PPTP (Point-to-Point Tunneling Protocol) is a protocol that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. Enable/Disable this protocol verification.
□L2TP Pass Through - L2TP (The Layer 2 Tunnel Protocol) is an emerging Internet Engineering Task Force (IETF) standard that combines the best features of two existing tunneling protocols: Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP is an extension to the Point-to-Point Protocol (PPP), which is an important component for VPNs. VPNs allow users and telecommuters to connect to their corporate intranets or extranets. Enable/Disable this function.
□SIP ALG - SIP, the Session Initiation Protocol, is a signaling protocol for Internet conferencing, telephony, presence, events notification and instant messaging. Enable/Disable this protocol verification.
□DMZ - In computer networks, a DMZ (Demilitarized Zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. Think of DMZ as the front yard of your house. It belongs to you and you may put some things there, but you would put anything valuable inside the house where it can be properly secured. Setting up a DMZ is very easy. If you have multiple computer s, you can choose to simply place one of the computers between the Internet connection and the firewall.
If you have a computer that cannot run Internet applications properly from behind the device, then you can allow the computer to have unrestricted Internet access. Enter the IP address of that computer as a DMZ host with unrestricted Internet access. Adding a client to the DMZ may expose that computer to a variety of security risks; so only use this option as a last resort.

Virtual Server Setting

The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network. You will only need to input the LAN IP address of the computer running the service and enable it.
A Virtual Server is defined as a service port, and all requests to this port will be redirected to the computer specified by the server IP.

□Enable - Enable/Disable the virtual server mapping, default setting is Disable.
□WAN Port - The port number on the WAN side that will be used to access the virtual service. Enter the WAN Port number, e.g. enter 80 to represent the Web(http server), or enter 25 to represent SMTP (email server). Note: You can *specify maximum 32 WAN Ports.*
□Protocol - The protocol used for the virtual service. Select a protocol type is TCP or UDP.

□LAN IP - The server computer in the LAN network that will be providing the virtual services. Enter the IP address of LAN.
□LAN Port - The port number of the service used by the Private IP computer. Enter the LAN port number.
□Action - Insert a new WAN port or update a specified WAN port.

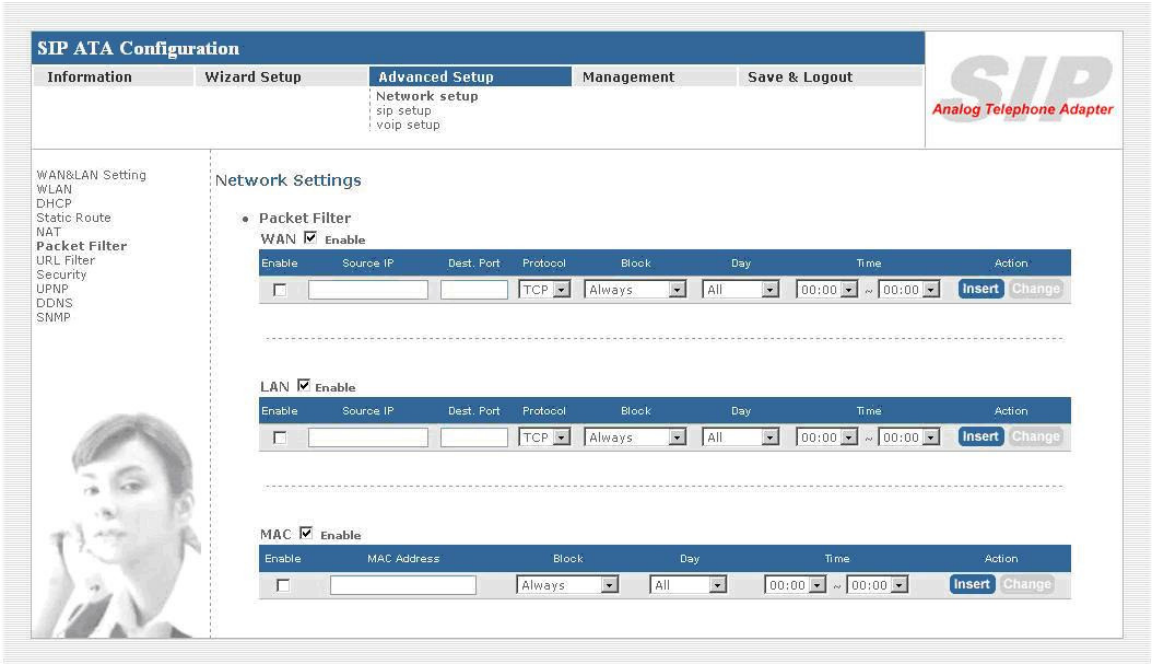
Port Trigger

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP (Transmission Control Protocol) or UDP (User Datagram Protocol), then enter the public ports associated with the trigger port to open them for inbound traffic.

□Enable - Enable/Disable the port trigger, default setting is Disable.
□Trigger Port - This is the port used to trigger the application. It can be either a single port or a range of ports.
□Trigger Type - This is the protocol used to trigger the special application.
□Public Port - This is the port number on the WAN side that will be used to access the application. You may define a single port or a range of ports. You can use a comma to add multiple ports or port ranges.
□Public Type - This is the protocol used for the special application.
□Action - Insert a new Port Trigger or update a specified Port Trigger.

3.7 PacKet Filter

Controlling access to a network by analyzing the incoming packets and letting them pass or halting them based on the IP addresses of the source.



□WAN Enable/Disable - The WAN IP port packet filter function ,control a network IP port ,default setting is Enable.
□Enable - Enable/Disable the Internet to WAN IP source port rules, default setting is Disable.
□Source IP - This is the filter WAN IP address.
Example: 209.131.36.158
□Dest. Port - This is the port used for source IP service.
□Protocol - This Protocol Used for the source IP service. Select a protocol type is TCP or UDP.
□Black - Wan IP Port Black time. Select a Always or by schedule.
□Day - Black day, Select a All / Mon-Sat./ Mon-Fri./Mon./ Tues./ Wed./Thu./Fri./Sat./Sun.
□Time – Black time, Select time range is 00:00 to 23:59.
□LAN Enable/Disable – Internet to LAN filter function ,default setting is Enable. A prohibitive rule set should only allow the necessary Internet/DMZ services to LAN (Local Area Network) clients.
□Enable - Enable/Disable the WAN IP source port rules, default setting is Disable.
□Source IP - This is the filter source IP address to LAN.
□Dest. Port - This is the port used for source IP.
□Protocol - This Protocol Used for the WAN Filter service. Select a protocol type is TCP or UDP
□Day - Black day, Select a All / Mon-Sat./ Mon-Fri./Mon./ Tues./ Wed./Thu./Fri./Sat./Sun.
□Time – Black time, Select time range is 00:00 to 23:59

□MAC Enable/Disable –Form internet MAC filter function ,default setting is Enable.
□Black - Wan IP Port Black time. Select a Always or by schedule.
□Day – Select Black day, Select a All / Mon-Sat./ Mon-Fri./Mon./ Tues./ Wed./Thu./Fri./Sat./Sun.
□Time – Black time, Select time range is 00:00 to 23:59

3.8 URL Filter

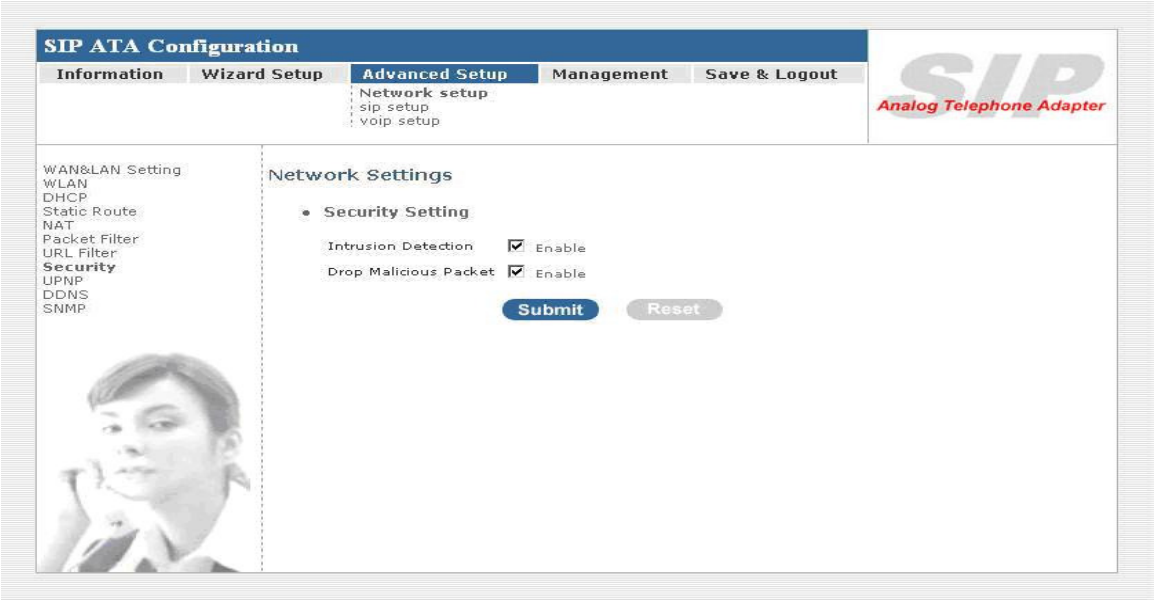
URL filter allows you to block sites based on a black list and white list. Sites matching the black list but not matching the white list will be automatically blocked and closed.

□Enable - Enable/Disable the URL filter function, default setting is Disable.
□Enable - Enable/Disable Block URL to the Clinet IP, default setting is Disable
□Client IP - This is the Clinet IP is LAN address.
Example: 222.222.222.100
□URL Filter String - This is the filter URL.
Example: “http://www.yahoo.com/”

3.9 Security

Intrusion Detection has powerful management and analysis tools that let your IT administrator see what's going on in your network. Such as who's surfing the Web, and gives you the tools to block access to inappropriate Web sites.

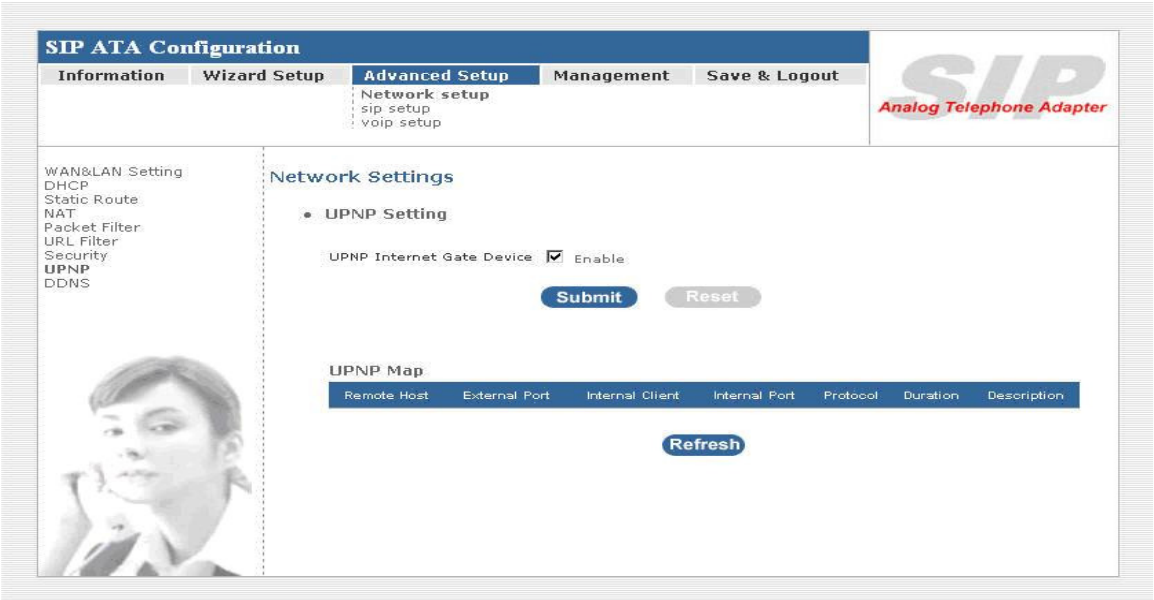
Malicious code (also called vandals) is a new breed of Internet threat that cannot be efficiently controlled by conventional antivirus software alone. In contrast to viruses that require a user to execute a program in order to cause damage, vandals are auto-executable applications.



□Intrusion Detection - Enable / Disable , network / internet security protection.
□Drop Malicious Packet - Enable / Disable , Detect and drop malicious application layer traffic.

3.10 UPNP

UPnP provides support for communication between control points and devices. The network media, the TCP/IP protocol suite and HTTP provide basic network connectivity and addressing needed. On top of these open, standard, Internet based protocols, UPnP defines a set of HTTP servers to handle discovery, description, control, events, and presentation.



□ UPNP Internet Gate Device – Enable/Disable UPNP Service to working ,default setting is Disable.

3.11 DDNS

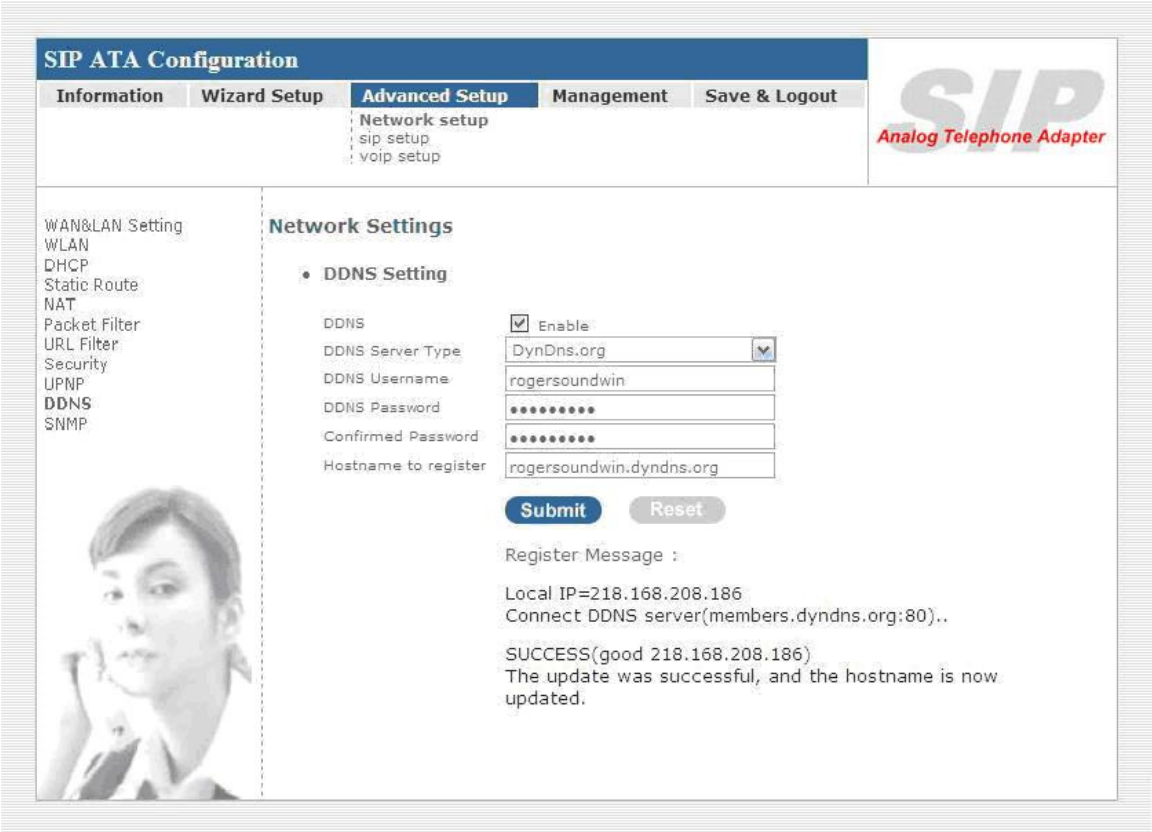
The DDNS (Dynamic DNS) service allows you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessed from various locations on the Internet.

Without DDNS, the users should use the WAN IP to reach internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported, you apply a DNS name (e.g., www.ata.com) for your server (e.g., Web server) from a DDNS server. The outside users can always access the web server using the www.ata.com regardless of the WAN IP.

When you want your internal server to be accessed by using DNS name rather than using the dynamic IP address, you can use the DDNS service. The DDNS server allows to alias a dynamic IP address to a static hostname.

Unlike DNS that only works with static IP addresses, DDNS works with dynamic IP addresses, such as those assigned by an ISP or other DHCP server. DDNS is popular with home networkers, who typically receive dynamic, frequently-changing IP addresses from their service provider.

DDNS is a method of keeping a domain name linked to a changing (dynamic) IP address. With most Cable and DSL connections, you are assigned a dynamic IP address and that address is used only for the duration of that specific connection. With the ATA, you can setup your DDNS service and the ATA will automatically update your DDNS server every time it receives a different IP address.

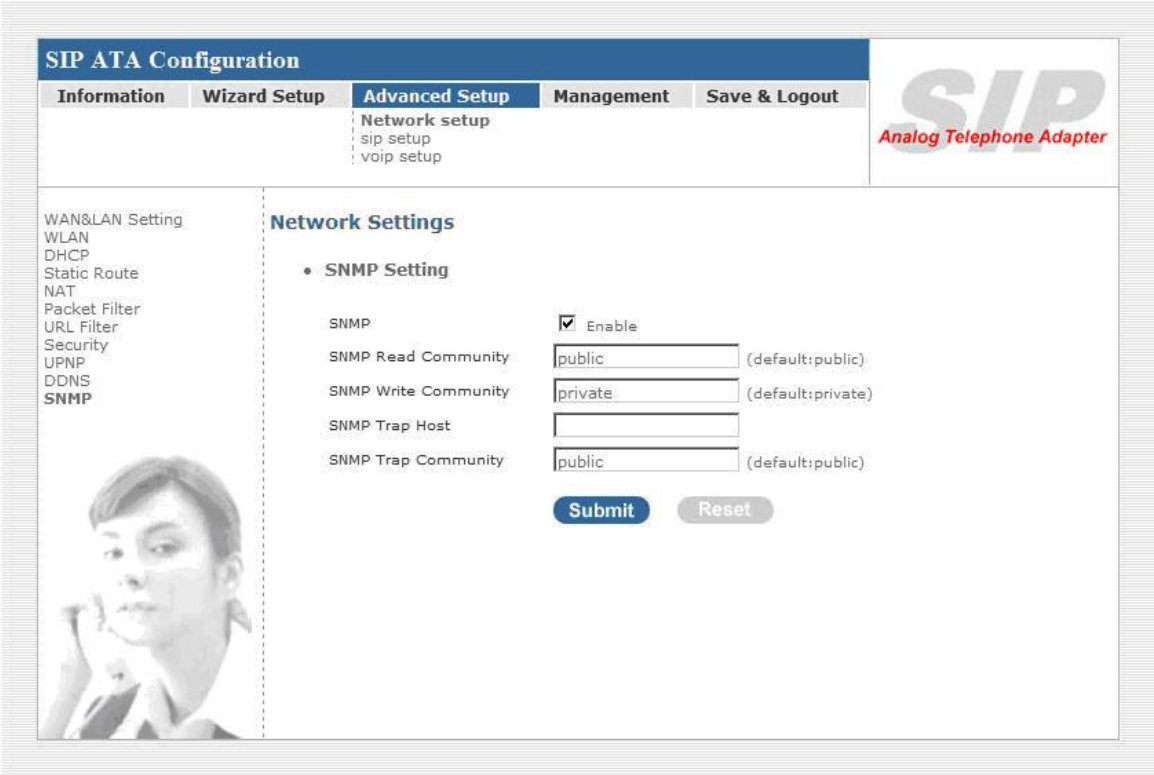


□Enable - Enable/Disable the DDNS service, default setting is Disable.
□DDNS Server Type - The ATA support two types of DDNS, DynDns.org or No-IP.com
□DDNS Username - The username which you register in DynDns.org or No-IP.com website.
□DDNS Password - The password which you register in DynDns.org or No-IP.com website.
□Confirmed Password - Confirm the password which you typing.
□Hostname to register - The hostname which you register in DynDns.org or No-IP.com website.

3.12 SNMP

The simple network management protocol (SNMP) forms part of the internet protocol suite as defined by the Internet Engineering Task Force (IETF). SNMP is used by network management systems to monitor network-attached devices for conditions that warrant administrative attention. It consists of a set

of standards for network management, including an Application Layer protocol, a database schema, and a set of data objects.

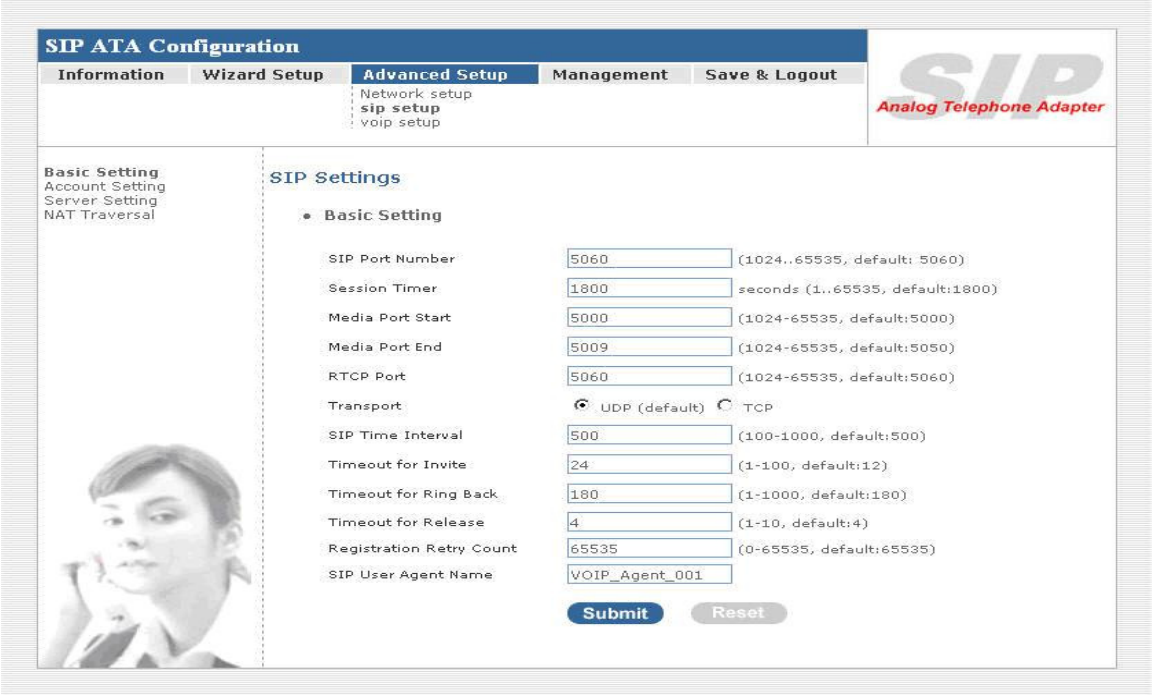


□Enable - Enable/Disable the SNMP service, default setting is Disable. (Support SNMP version 1 or SNMP version 2c).
□SNMP Read Community - SNMP Read Community string so that EPICenter can retrieve information.(default :public)
□SNMP Write Community - Specifies the name of the SNMP write community to which the printer device that this actual destination represents belongs.(Default:private)
□SNMP Trap Host - Defines an SNMP trap host to which AppCelera will send trap messages. (Default address is empty)
□SNMP Trap Community –The SNMP trap community name. The community name functions as a password for sending trap notifications to the target SNMP manager.(Default : public).

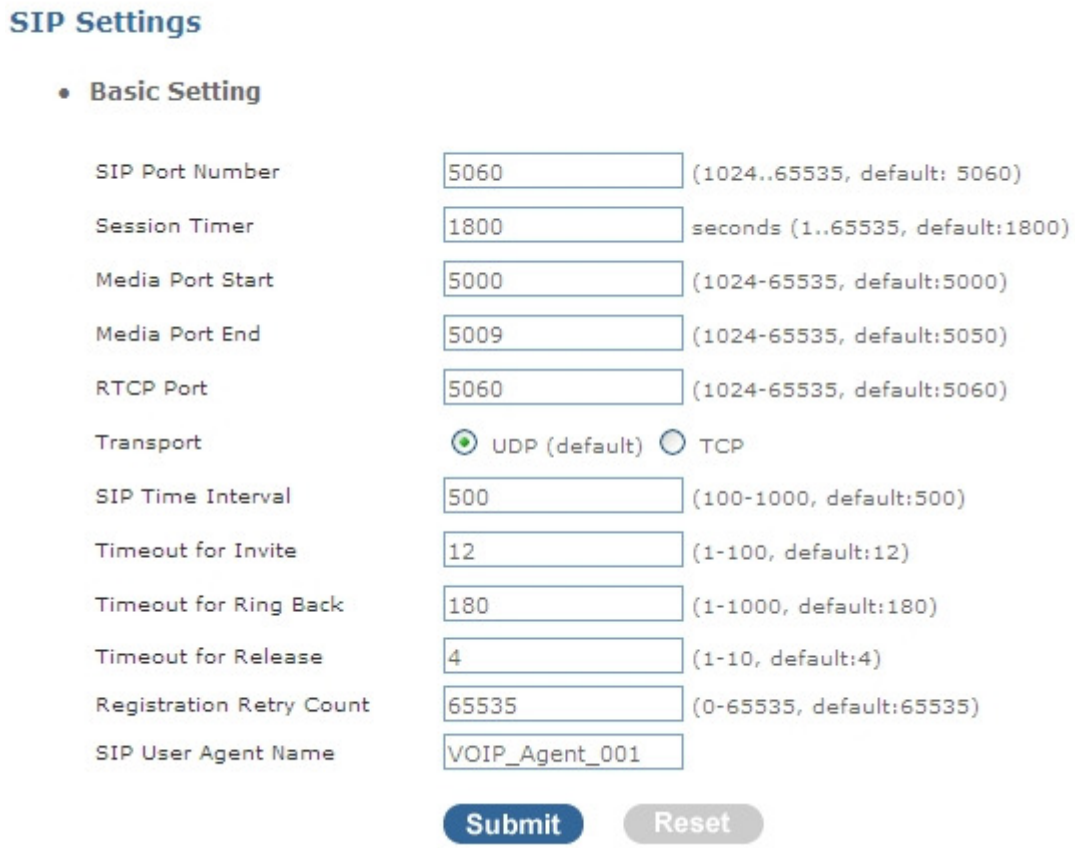
SIP Setting

SIP is a request-response protocol, dealing with requests from clients and responses from servers. Participants are identified by SIP URLs. Requests can be sent through any transport protocol. SIP determines the end system to be used for the session, the communication media and media parameters, and the called party's desire to engage in the communication. Once these are assured, SIP establishes call parameters at either end of the communication, and handles call transfer and termination.

- Basic Setting
- Account Setting
- Server Setting
- NAT Traversal



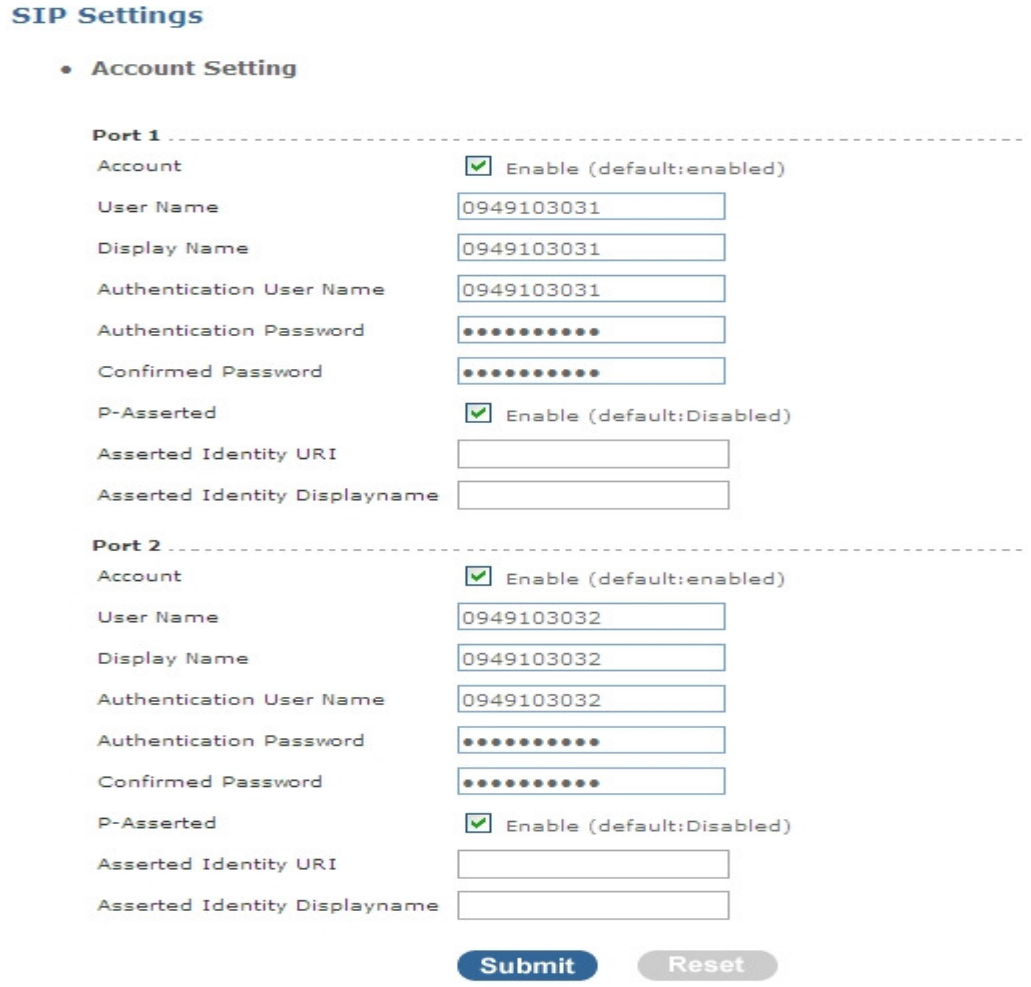
4.1 Basic Setting


SIP Settings
Basic Setting
SIP Port Number 5060 (1024..65535, default: 5060)
Session Timer 1800 seconds (1..65535, default:1800)
Media Port Start 5000 (1024-65535, default:5000)
Media Port End 5009 (1024-65535, default:5050)
RTCP Port 5060 (1024-65535, default:5060)
Transport UDP (default) TCP
SIP Time Interval 500 (100-1000, default:500)
Timeout for Invite 12 (1-100, default:12)
Timeout for Ring Back 180 (1-1000, default:180)
Timeout for Release 4 (1-10, default:4)
Registration Retry Count 65535 (0-65535, default:65535)
SIP User Agent Name VOIP_Agent_001
Submit
Reset

□SIP Port Number - Assign the SIP port number of Telephone adapter. Its range is 1024 to 65535, default setting is 5060.
□Session Timer - SIP session refresh time interval. The time interval in which the phone periodically refresh SIP sessions by sending repeated INVITE or Update request, depending on session type. Its

range is 1 to 65535, default setting is 1800 seconds.
□Media Port Start - The starting range of port for RTP. Port number for initial of sending RTP packet. Its range is 1024 to 65535, default setting is 5000.
□Media Port End - The ending range of port for RTP. Its range is 1024 to 65535, default setting is 5050.
□RTCP Port - The Real Time Transport Control Protocol (RTP control protocol or RTCP) is based on the periodic transmission of control packets to all participants in the session, using the same distribution mechanism as the data packets. The underlying protocol must provide multiplexing of the data and control packets, for example using separate port numbers with UDP. Assign the RTCP port number of Telephone adapter. Its range is 1024 to 65535, default setting is 5060.
□Transport - Assigns the default SIP transport protocol.
 UDP - UDP (User Datagram Protocol) provides very few error recovery services, offering instead a direct way to send and receive datagram over an IP network. It's used primarily for broadcasting messages over a network. Here the UDP is a default setting.
 TCP - TCP (Transmission Control Protocol) guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.
□SIP Time Interval - SIP time interval in milliseconds. The default setting is 500 m-sec.
□Timeout for Invite - INVITE message timeout value. Assigns a value 1 to 100, default setting is 12 seconds. It denotes if an INVITE request was sent, and a response is not received from the remote site within the allotted time (the value of Invite Timeout). The present request will be dropped and a new connection request will be initiated.
□Timeout for Ring Back - Timeout value for dropping a call after receiving 180 responses. Ring back is an intermittent audio tone that a caller in a telephone system hears after dialing a number, when the distant end of the circuit is receiving a ringing signal. It can be generated by the servicing switch of either the called party or the calling party. It is not generated by the called instrument. The default setting is 180 seconds.
□Timeout for Release - BYE message timeout value. Assigns a time interval 1 to 4, default setting is 4 seconds.
□Registration Retry count - Assigns a value 1 to 65535 ,To set the retry count for keepalive retransmission, use the retry keepalive command in SIP user agent configuration mode. To restore the retry count to the default value for keepalive retransmission, use the no form of this command.
□SIP User Agent name - if specfied, is the user-agent name to be used in a REGISTER request. If not specified, the value in”SIP User Agent Name” will be used for REGISTER request also. Default value is VOIP_Agent_001.

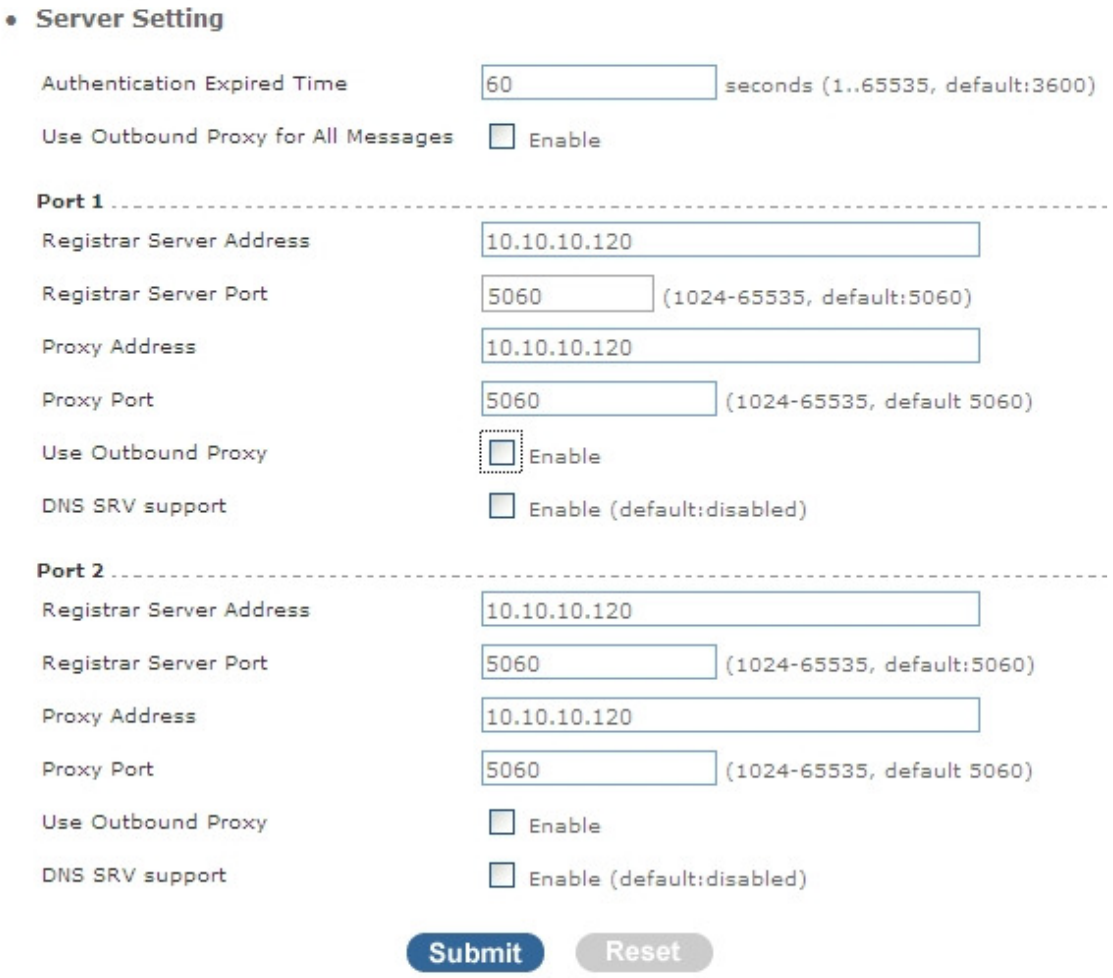
4.2 Account Setting



There are two ports can be setup for SIP account.
□Phone Number - Assigns Phone number for the first port, maximum 15 digits. Do not contain any special characters or spaces. E.g. if you want to enter the number +886 2 2788-8118, then it should be 886227888118.
□Display Name - This text message will be sent between the callee and caller and will show on LCD panel for general using.
□Authentication User Name - User name for authentication. Maximum 36 characters.
□Authentication Password - User password for authentication. Maximum 24 characters.
Confirmed Password - Enter the password again, this is used to confirm user password for authentication. Maximum 24 characters.
□P-Asserted - Enable/Disable . Support for the Remote-Party-ID header and P-Asserted-Identity header—The present SIP implementation always derives the calling party number from the user name field of From header. But if P-Asserted-Identity header or Remote-Party-ID header is present in an incoming SIP INVITE message the user name should be derived from those headers.
□Asserted Identity URI – Enter your URI (Uniform Resource Identifier), Maximum 24 characters.
□Asserted Identity Displayname - Enter your Display name, Maximum 24 characters.

4.3 Server Setting

SIP Settings

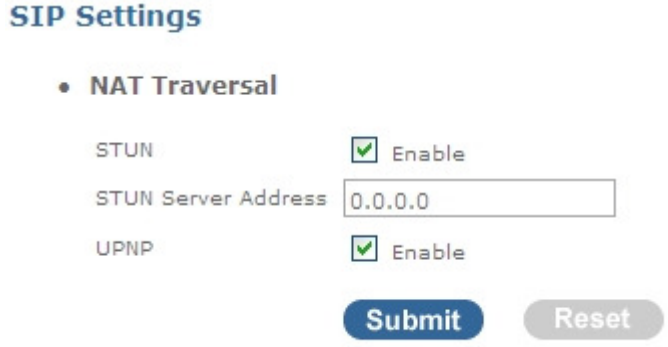


□Authentication Expired Time - SIP registration expired time. Assigns the time interval from 1 - 65535, default setting is 3600 seconds.
□Use Outbound Proxy for All Messages - Enable/Disable this flag for out-bound (out-session and in-session) requests. Default setting is Disable.
□Registrar Server Address - Assigns the SIP Register Server's IP address.
□Registrar Server Port - Port number of SIP Register Server. Assigns a value from 1024 to 65535, default setting is 5060.
□Use Outbound Proxy for Session - Enable/Disable this flag for proxy-outbound, default setting is Disable.
□Outbound Proxy Address - Outbound Proxy server's IP address. Assigns the server's IP which is in charge of call-out service.
□Outbound Proxy Port - Port number of Outbound Proxy Server. Assigns a number from 1024 to 65535, default setting is 5060.
□DNS SRV support – Enable/Disable DNS SRV support function,You'll need DNS server if you want to use email server. To use it you should check Direct delivery on the addresses tab. DNS server is used to give a route to recipients' mailbox. You can use any DNS you know. But the best choice for the fastest sending is to use your ISP's DNS.

4.4 NAT Traversal

STUN (Simple Traversal of UDP through NATs (Network Address Translation)) is a protocol for assisting devices behind a NAT firewall or router with their packet routing.
STUN enables a device to find out its public IP address and the type of NAT service its sitting behind.

When you enable the STUN function, you must input the STUN server address.

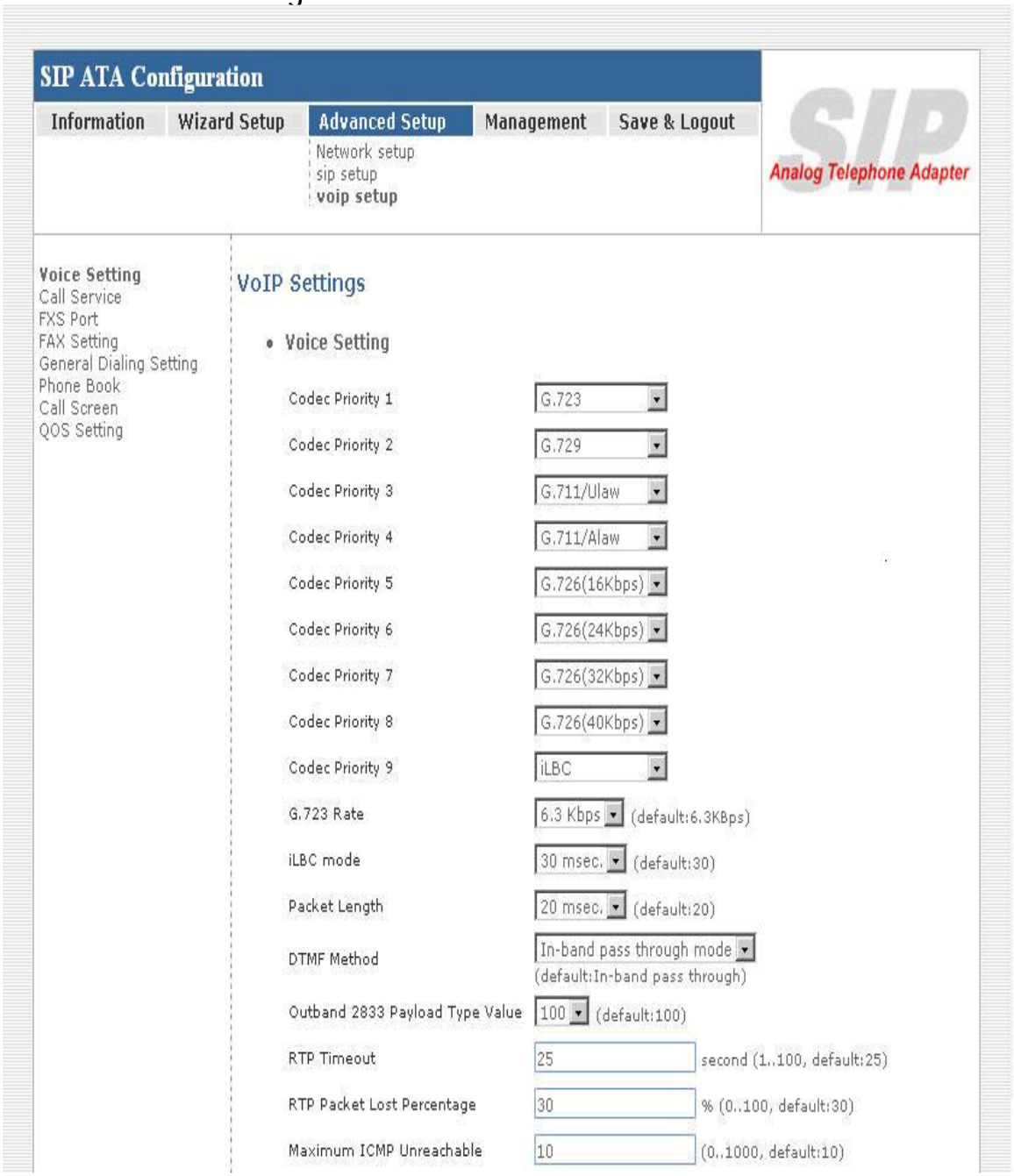


□UPNP – Enable/Disable Universal Plug and Play , default setting is Disable.

VoIP Setting

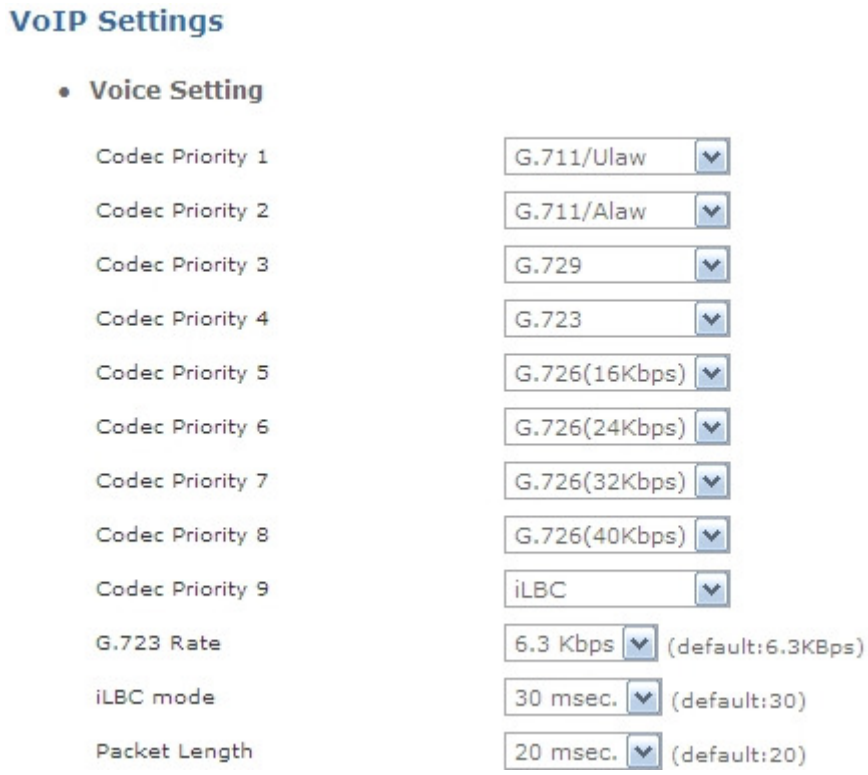
- Voice Setting
- Call Service
- FXS Port
- FAX Setting
- General Dialing Setting
- URI Phone Book
- Call Screen
- QOS Setting

5.1 Voice Setting



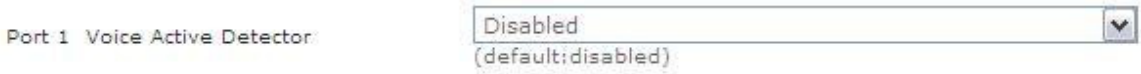
Codec

A CODEC (COmpressor/DECompressor) is an algorithm for taking voice or video and compressing the information. This type of codec combines analog-to-digital conversion and digital-to-analog conversion functions in a single chip. The Codec is used to compress the voice signal into data packets. Each Codec has different bandwidth requirement. There are 9 kinds of codec, G.711/Ulaw, G.711/Alaw, G.729, G.723, G.726(16K bps), G.726(24K bps), G.726(32K bps), G.726(40K bps), and iLBC.



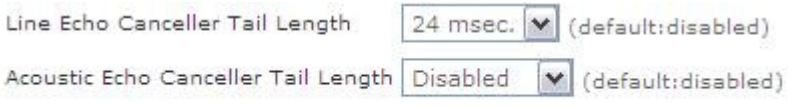
□Codec Priority 1~9 - The Codec is used to compress the voice signal into data packets. Each Codec has different bandwidth requirement. There are 9 kinds of codec. To determine the priority, selects one codec algorithm from the pull-down menus individually.
□G.723 Rate –This defines the encoding rate for G723 Codec(6.3Kbps/5.3Kbps), default is 6.3Kbps Rate.
□ILBC Mode - RTP Payload length. Select a length from the pull-down menu, default setting is 30 m-sec.
□Packet Length - RTP payload length. Selects a length from the pull-down menu, default setting is 20 m-sec.

Voice Active Detector



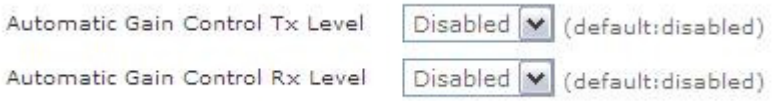
□Voice Active Detector - It is used in speech encoding software to determine if the voice being encoded is human speech or background noise. There are three type of silence suppression: NO CNG, Only G.711 Annex II type, and Codec Specific CN.

Echo Canceller



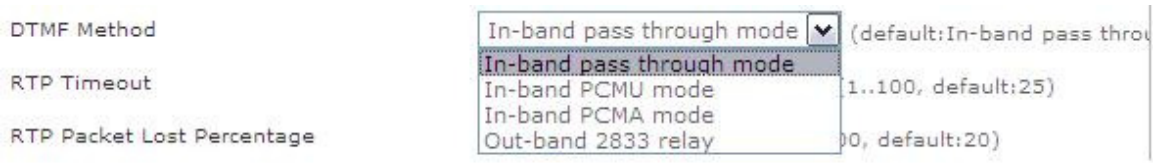
The echo canceller literally removes your voice from the returning audio stream without removing the audio coming from your caller.
□Line Echo Canceller Tail Length - Tail length for line echo cancellation. Default setting is in Disable mode.
□Acoustic Echo Canceller Tail Length - Tail length for acoustic echo cancellation. Default setting is in Disable mode.

Gain Control Level



You can adjust the FXO Tx/Rx Gain Control level, range from 0db to 30db. The “gain” means increase in the power of electrical signal, measures by decibel.
□Automatic Gain Control Tx Level - Automatic voice gain control for transmitting. Default setting is in Disable mode.
□Automatic Gain Control Rx Level - Automatic voice gain control for receiving. Default setting is in Disable mode.

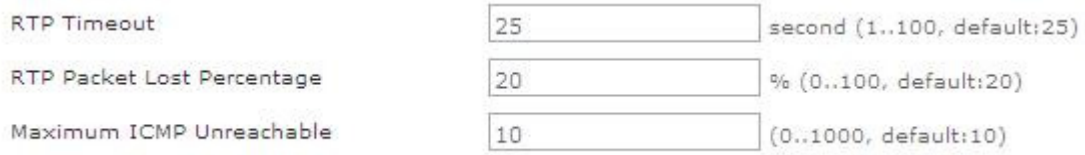
DTMF Method



After the VoIP call is connected, when you dial a digit, this digit is sent to the other side by DTMF tone. There are two methods of sending the DTMF tone, In-band and Out-band. Choose “I n-band” will send the DTMF tone in voice packet. Choose “Out-band” will send the DTMF tone as a RTP payload signal. Sending DTMF tone as a signal could tolerate more packet loss caused by the network. If this selection is enabled, the DTMF tone will be sent as a signal.
□DTMF Method - Select the DTMF relay method, default setting is In-band pass through mode.
◎In-band - For voice data. The In-band signaling is the sending of metadata and control information in the same channel used for data. There are three type of mode can be selected: In-band pass through mode, In-band PCMU mode, and In-band PCMA mode.
◎ Out-band - For RFC-2833, that is, sending the DTMF tone as a RTP payload signal. The Out-of-band signaling has the following meanings:
1. Signaling that uses a portion of the channel bandwidth provided by the transmission medium, e.g., the carrier channel, which portion is above the highest frequency used by, and is denied to, the speech or intelligence path by filters.
Note: Out-of-band signaling results in a lowered high-frequency cutoff of the effective available bandwidth.
2. Signaling via a different channel (either FDM or TDM) from that used for the primary information transfer.

RTP

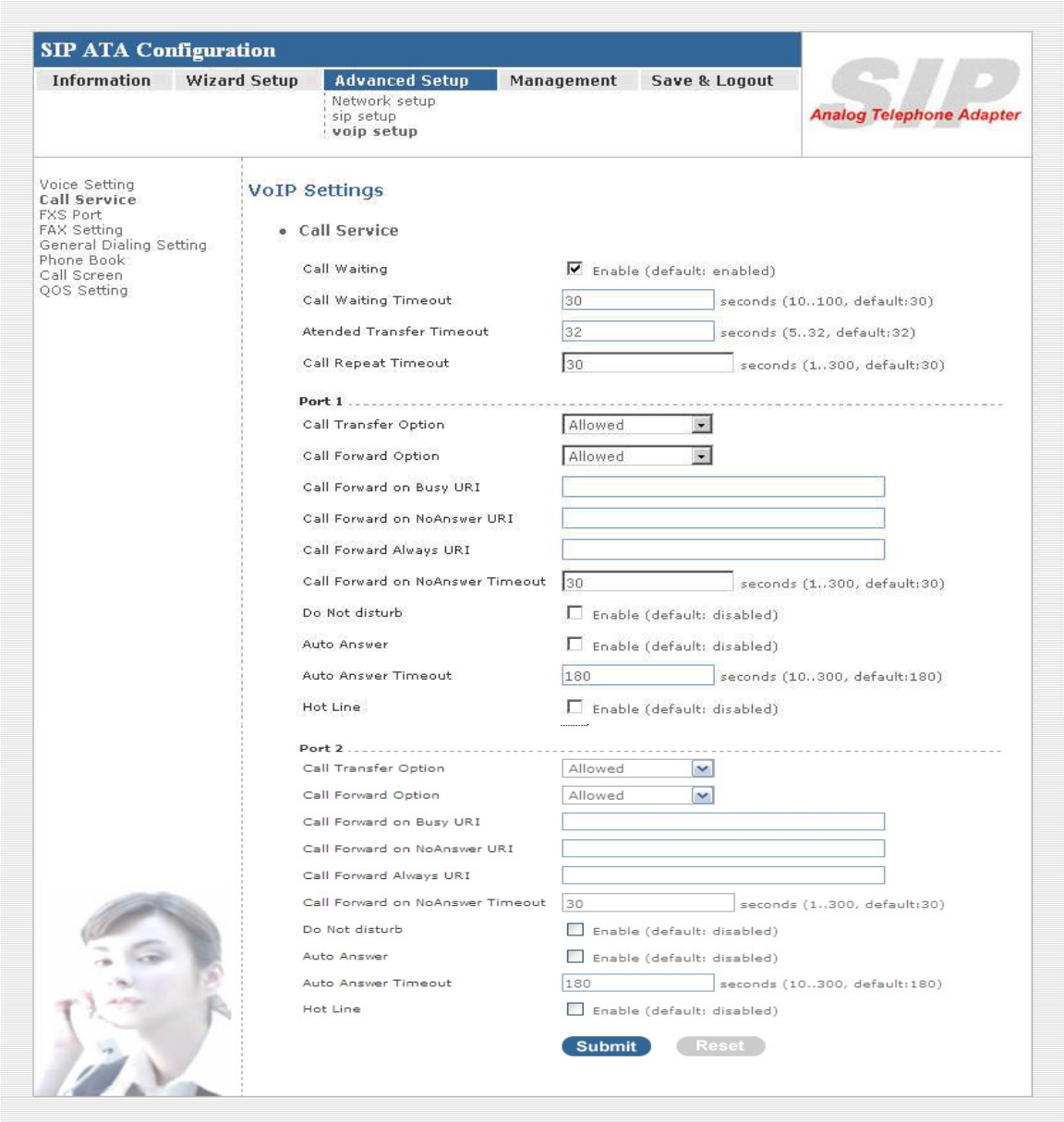
RTP provides end-to-end network transport functions suitable for applications transmitting real-time data, such as audio, video or simulation data, over multicast or unicast network services. RTP does not address resource reservation and does not guarantee quality-of-service for real-time services. The data transport is augmented by a control protocol (RTCP) to allow monitoring of the data delivery in a manner scalable to large multicast networks, and to provide minimal control and identification functionality. RTP and RTCP are designed to be independent of the underlying transport and network layers. The protocol supports the use of RTP-level translators and mixers.



□RTP Timeout - Disconnect a call after not receiving RTP packet for this time value. Assigns the time value from 1 to 100, default setting is 25 seconds.
□RTF Packet Lost Percentage - Allowable the maximum percentage of RTP packet loss. Assigns the percentage from 0 to 100, default setting is 20%

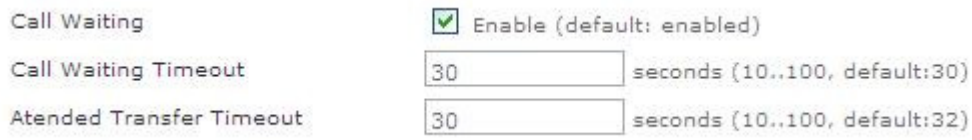
□Maximum ICMP Unreachable - Allowable the maximum number of consecutive ICMP destination unreachable responses. ICMP differs in purpose from TCP and UDP in that it is usually not used directly by user network applications. One exception is the ping tool, which sends ICMP Echo Request messages (and receives Echo Response messages) to determine whether a host is reachable and how long packets take to get to and from that host. Assigns a number from 10 to 100, default setting is 10.

5.2 Call Service



Call Waiting

It is a feature on telephone network. If a calling party places a call to a called party which is otherwise engaged, and the called party has the call waiting feature enabled, the called party is able to suspend the current telephone call and switch to the new incoming call, and can then negotiate with the new or the current caller an appropriate time to ring back if the message is important, or to quickly handle a separate incoming call.



□Call Waiting - The default setting is Enable mode.
□Call Waiting Timeout - Assigns the time interval from 10 to 100. Default setting is 30 seconds.
□Attended Transfer Timeout - Assigns the time interval from 10 to 100. Default setting is 30 seconds.

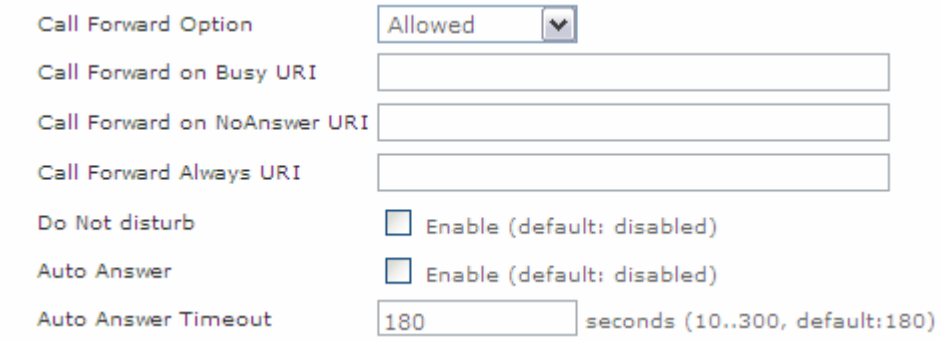
Call Transfer Option

The Call Transfer Option feature which can enables a user to relocate an existing call to another telephone or attendants console by using the transfer button then dialing the required location. The transferred call is either announced or unannounced.

□Call Transfer Option - Indicates whether the remote end is allowed to transfer the call to a third party. There are three type, Restricted, Allowed, and User Invocation Required. The default setting is in Allowed mode.

Call Forward Option

The Call Forwarding Option is a feature on telephone network that allow an incoming call to a called party which would be otherwise unavailable to be redirected to a mobile telephone or other telephone number where the desired called party is situated.

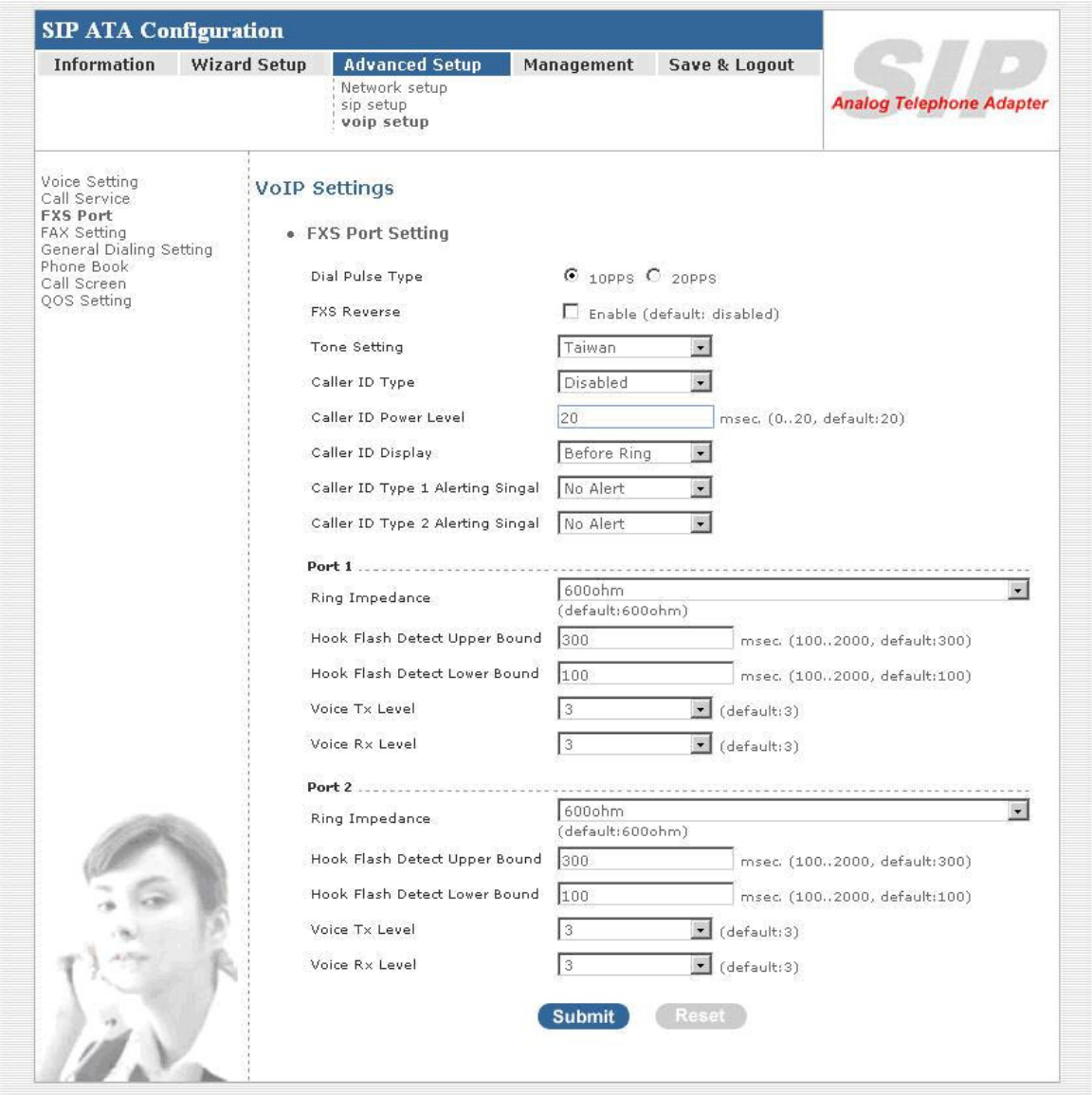


□Call Forward Option - Indicates whether the remote end is allowed to forward the call to a third party. There are three type, Restricted, Allowed, and User Invocation Required. The default setting is in Allowed mode.
□Call Forward on Busy URI - Assigns a phone number. When the port is busy, the incoming call will be redirected to the specified phone number.
□Call Forward on No Answer URI - Assigns a phone number. When the port is no answer, the incoming call will be redirected to the specified phone number.
□Call Forward Always URI - Assigns a phone number; if you want all incoming calls of the port always be redirected.
□Do Not disturb - Enable/Disable the do not disturb, default setting is disabled.
□Auto Answer - Enable/Disable the auto answer, default setting is disabled.
□Auto Answer Timeout - When the phone is ring a long time (180 seconds), the incoming call will timeout and redirected to the specified phone number which is fill in “Call Forward on No Answer URI”. Default setting is 180 seconds.

□Hot line - Enable/Disable , default setting is disable, This service allows you to make a call to a pre-programmed number by only lifting the handset.

5.3 FXS Port Setting

FXS (Foreign Exchange Station) is the interface on a VoIP device for connecting directly to telephones, fax machines, or similar device and supplies ring, voltage, and dial tone.



□Dial Pulse Type - This field defines the number of pulse per second. There are 2 selections,

◎10 PPS - Represents as a series of audible clicks of 16.66 ms duration with silence duration of 33.33 ms.

◎20 PPS - Represents as a series of audible clicks of 33.33 ms duration with silence duration of 66.66 ms.

Note: These values apply to the Japanese Network for which the algorithm was developed.

These click sounds are digitized and subsequently analyzed to determine the digit that was dialed.

□FXS Reverse - A specific signal indicating the status of the conversation.

□Tone Setting - Adjust the tone frequency according to each country. Select a country from the pull-down menu.

□Caller ID Type - The Caller ID normal display the number, system date, and time on system phone screen of the incoming call. The DTMF is the general type for using. Select a type from the pull-down menu. Default setting is Disabled.

□Caller ID Power Level - Assigns the Caller ID Power Lever from 0 to 100. Default setting is 20 m-secs.

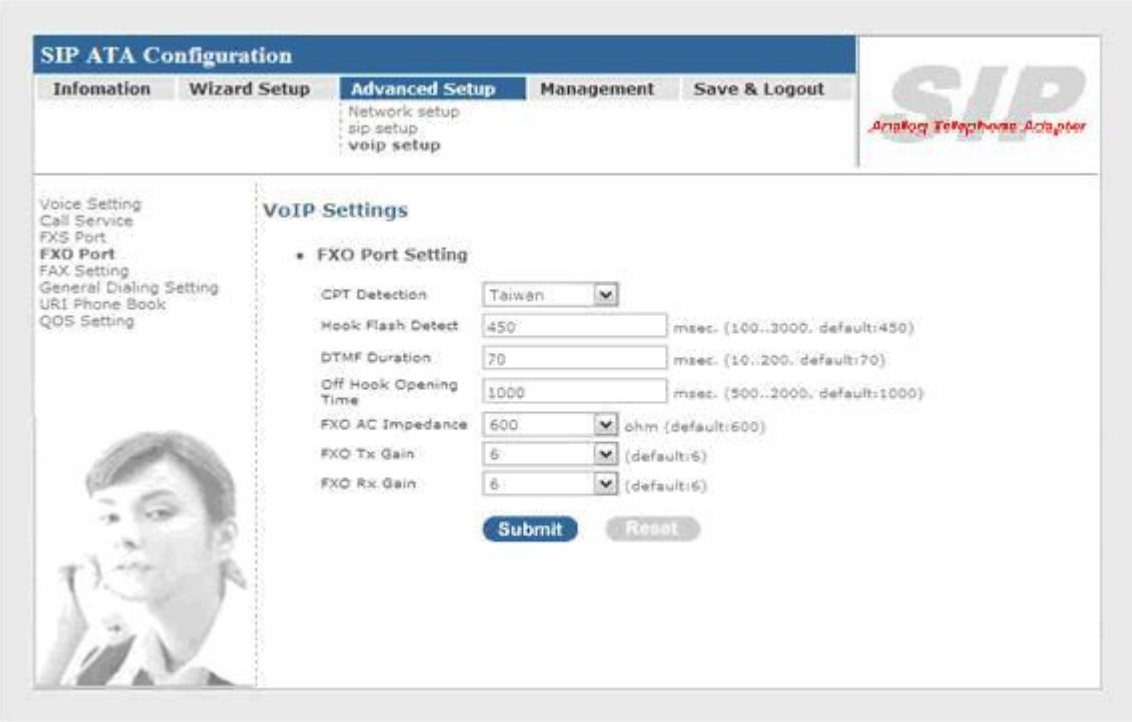
□Caller ID Display - There are two types to display the caller information on the screen. Before Ring, the caller id information is displayed before first ring. After Ring, the caller id information is displayed between first ring and second ring. Default setting is Before Ring.
□Caller ID Type 1 Alerting Signal - Type 1 alerting signal is used to detect CID when □device is ON-HOOK. Default setting is No Alert.
□Caller ID Type 2 Alerting Signal - Type 2 alerting signal is used to detect CID when device is OFF-HOOK. Default setting is No Alert.
□Hook Flash Detect - Hook-flash indicates the condition when a request for voice conference and is recognized as a quick off-hook/on-hook/off-hook cycle. Assign a time interval for Hook-flash detection from 100 to 2000; default setting is 300 m-secs.
□Voice Tx Level - Sets a specific sound intensity for transmitting sound. Select a level from 1 to 8, default setting is 6. Table1 lists the receive/transmit voice gain value for reference. The “gain” means increase in the power of electrical signal, measures by decibel.
□Voice Rx Level - Sets a specific sound intensity for receiving sound. Select a level from 1 to 8, default setting is 6. Table 1 lists the receive/transmit voice gain value for reference. The “gain” means increase in the power of electrical signal, measures by decibel.

Table 1 Receive/Transmit Voice Gain Value

Level	Decibel
1	-24db
2	-18db
3	-12db
4	-6db
5	-2.5db
6	0db(default setting)
7	3.5db
8	6db

5.4 FXO Port Setting(for 065-9056)

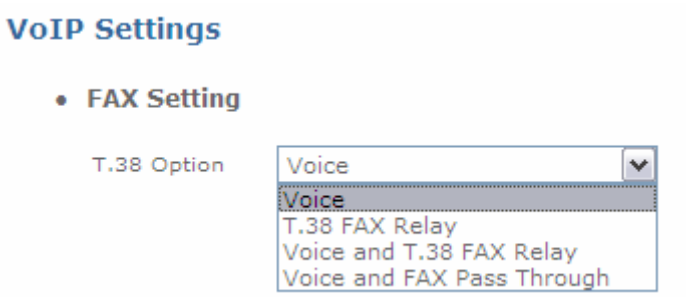
FXO(Foreign Exchange Office) is the interface on a VoIP device for connecting directly to PSTN CO Line, PBX Extension Line, or similar device and output ring, voltage, and dial tone.



□CPT Detection –Call Progress Tone Detection, Different country or PSTN/PBX device have different Tone, there are some country setting build in ATA, select country to setting Tone detection. Default country include in Taiwan/China/Japan/US.
□Hook Flash Detect –Hook-flash indicates the condition when a request for voice conference and is recognized as a quick off-hook/on-hook/off-hook cycle. Assign a time interval for Hook-flash detection from 100 to 3000; default setting is 300 m-secs.
□DTMF Duration – Input DTMF Duration time. Assign a time interval for DTMF Duration from 10 to 200, default setting is 70 m-sec.
□Off Hook Opening Time – Off Hook Opening time indicates the condition when a request for voice conference and is recognized as off-hook cycle. Assign a time interval for Off Hook Opening Time detection from 500 to 2000, default setting is 1000 m-sec.
□FXO AC Impedance –The FXO provides wild and complex ac termination impedances for selection.600/900/complex can be change. Default value is 600 ohm.
□FXO Tx Gain –Sets a specific sound intensity for transmitting sound. Select a level from 1 to 8, default setting is 6. Table1 lists the receive/transmit voice gain value for reference. The “gain” means increase in the power of electrical signal, measures by decibel.
□FXO Rx Gain –Sets a specific sound intensity for receiving sound. Select a level from 1 to 8, default setting is 6. Table 1 lists the receive/transmit voice gain value for reference. The “gain” means increase in the power of electrical signal, measures by decibel.

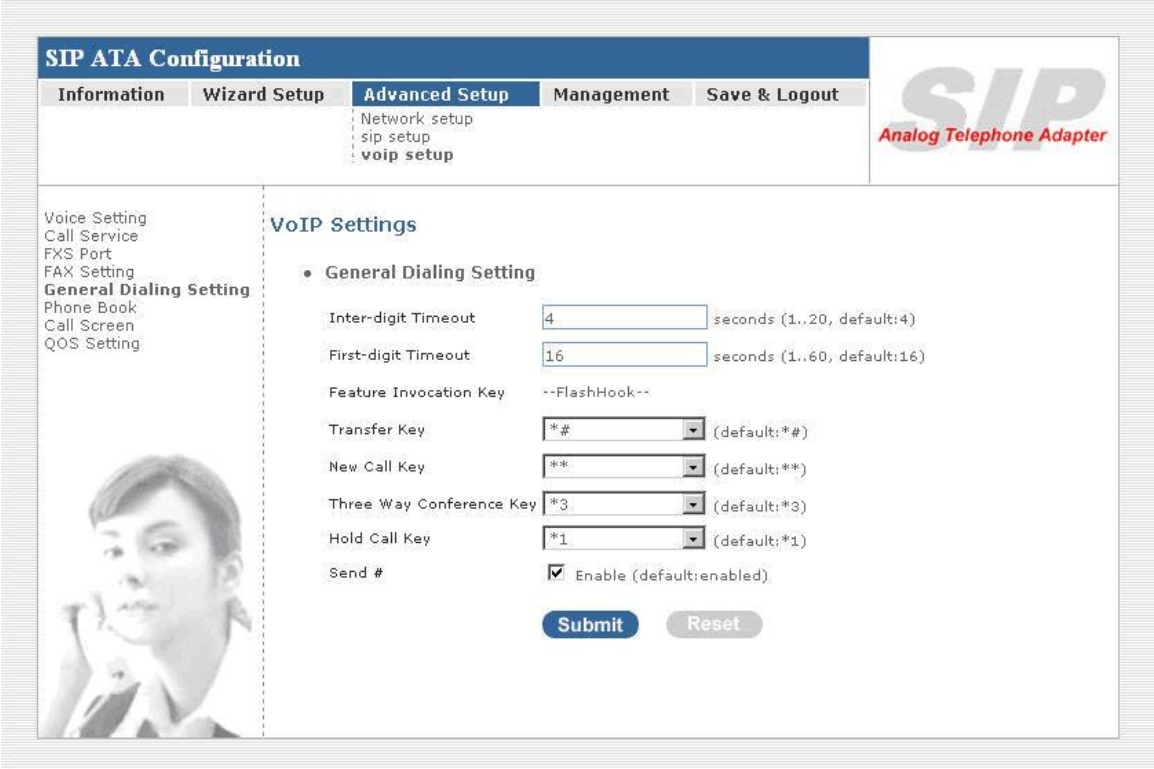
5.5 FAX Setting

The T.38 FAX procedure is used for the changeover from VoIP to fax mode during a call. The SIP will establish a normal VoIP call using INVITEs with SDP field to support T.38 detail.



□T.38 Option - Select an option from the pull-down menu. Default setting is Voice.

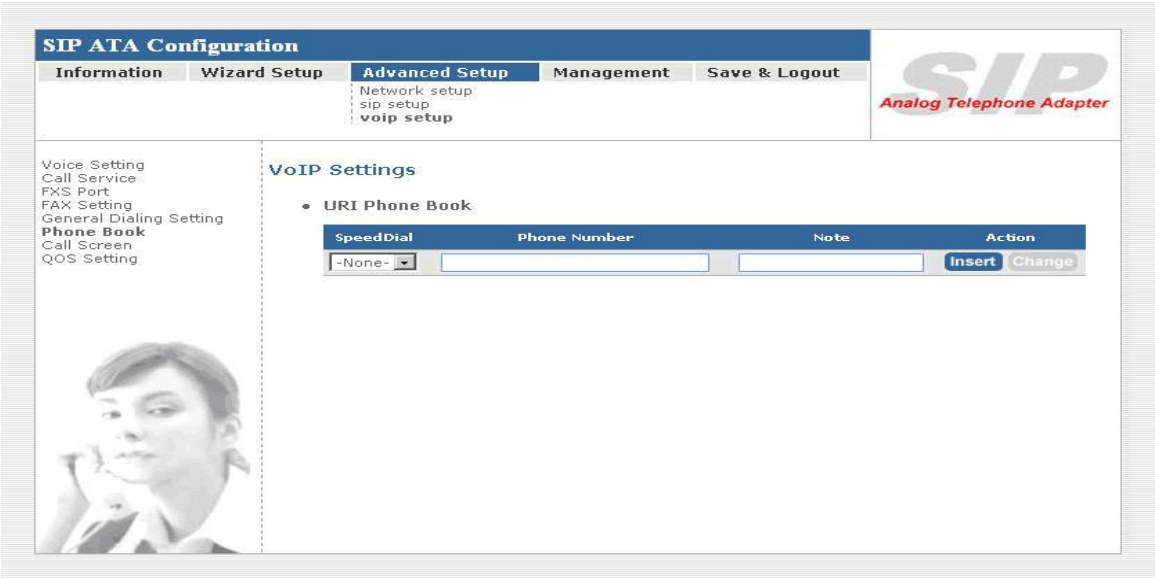
5.6 General Dialing Setting



□Inter-digit Timeout - If no other number is being dialed within this interval, the Telephony ATA will terminate this call. Assign the time interval from 1 to 20, default setting is 4 seconds.
□First-digit Timeout - If you pick up the phone without dialing any number within this period of time, the tone will be changed to busy tone. Assign the time interval from 1 to 60, default setting is 16 seconds.
□Feature Invocation Key - Key to invocate the other features. The setting is FlashHook key.
□Transfer Key - Keys to be pressed to initiate a call transfer. This is activated when
□HOLD/FLASH-HOOK is pressed on a call. The default setting is *#.
□New Call Key - Keys to be pressed to initiate a new call. The default setting is **.
□Three Way Conference Key - Keys to be pressed to initiate a 3-way conference call. The default setting is *3.
□Hold Call Key - Keys to be pressed will be holding a call. The default setting is *1.
□Send # - Enable/Disable , Default is Enable. speed dial ,after final dial don't need wait inter-digit time.

5.7 Phone Book

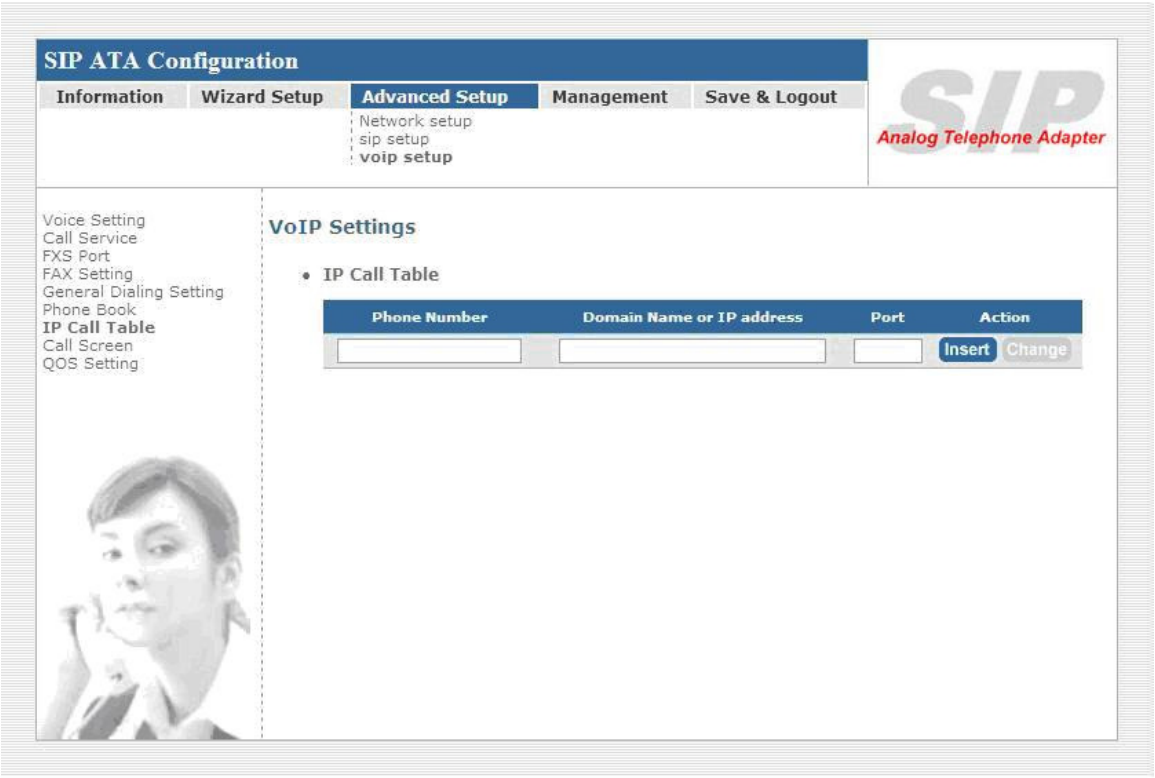
URI (Uniform Resource Identifier) Phone Book lets you define a button or a set of buttons to link to a specific number defined in URI Phone Book.



□SpeedDial - Select the speed dial shortcut to use from #1 to #9.
□Phone Number - Enter the international number to dial.
□Note – Phone munber note.

5.8 IP Call Table

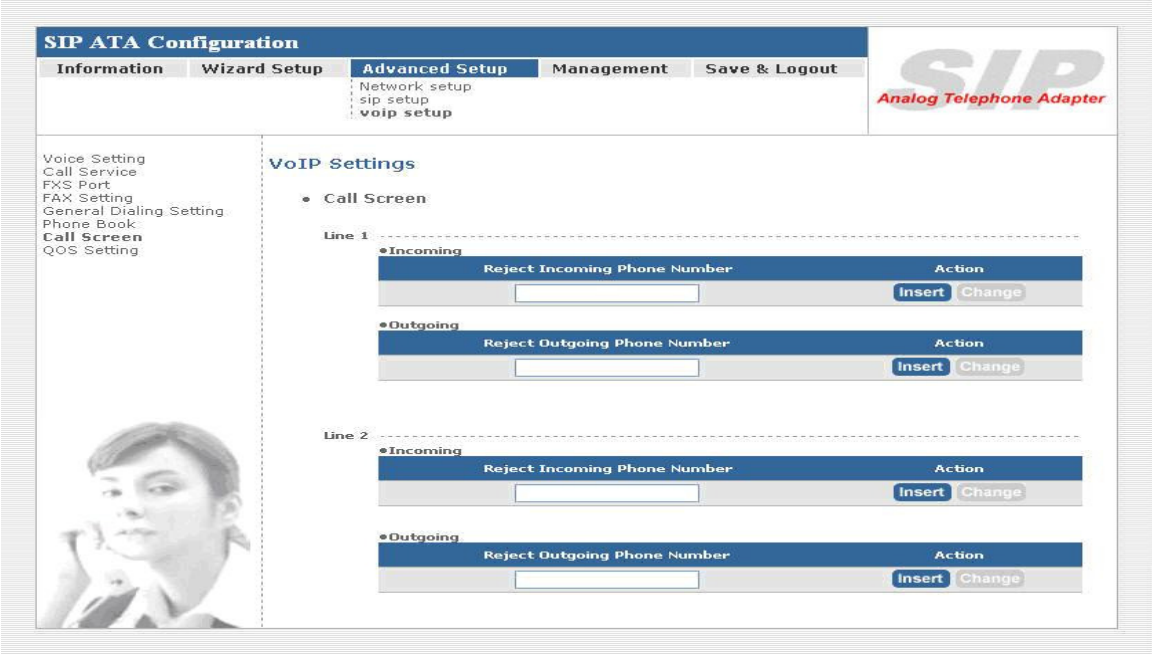
If you Want to make call to another SIP based internet Phone or peer to peer phone call , by using remote IP address, you can click "IP Call Table" then enter the Phone number and IP address.



□Phone Number – Enter remote call Phone number .
□Domain Name or IP address – Enter remote Phone IP Address or domain name..
□Port - Assign the remote SIP port number of Telephone adapter. Its range is 1024 to 65535, default setting is 5060

5.9 Call Screen

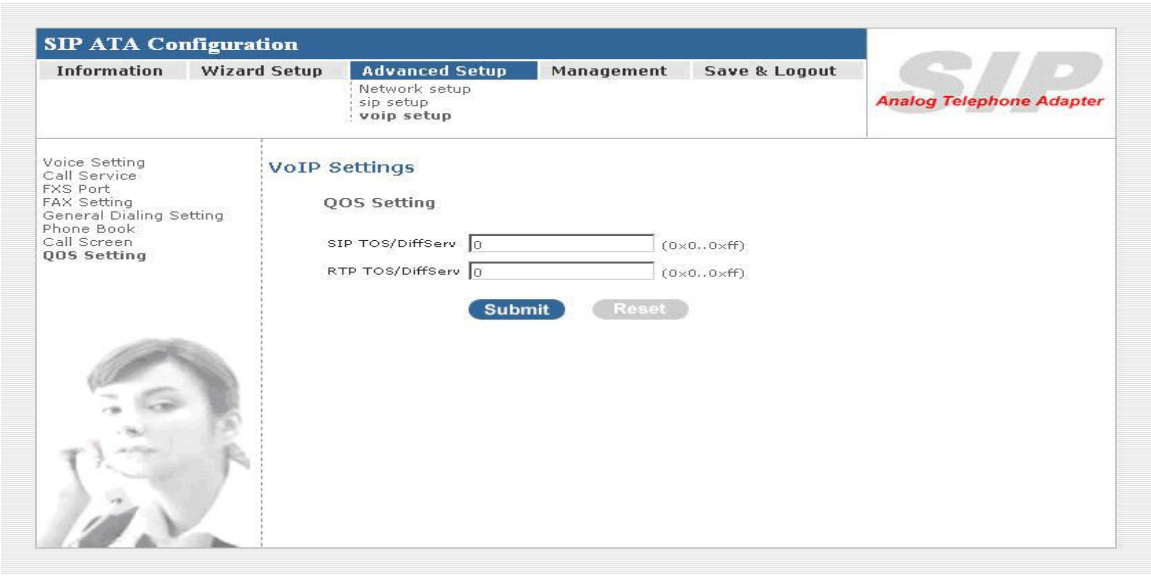
Call Screen allows you to block incoming or block outgoing calls from international number.



□Reject Incoming Phone Number - . Create and maintain a list of numbers to be screened. Incoming calls from the "screened callers" list will be blocked.
□Reject Outgoing Phone Number - . Create and maintain a list of numbers to be screened. Reject Outgoing Phonne nember from local user dial number.

5.10 QOS Setting

The QOS (Quality Of Service) is to guarantee that the Voice and Data should be transmitting at the same time and Data couldn't influence the Voice quality. When TOS bits is enabled, it will guarantee the Voice have the first priority pass through the TOS enable devices.



□SIP TOS/Diffserv – Set to value
□SIP TOS/Diffserv – Set to value

tos=0x10 low delay

tos=0x08 high throughput

tos=0x04 high reliability

tos=0x02 ECT bit set

tos=0x01 CE bit set

or set multiple bits, such as

```
tos=0x18
```

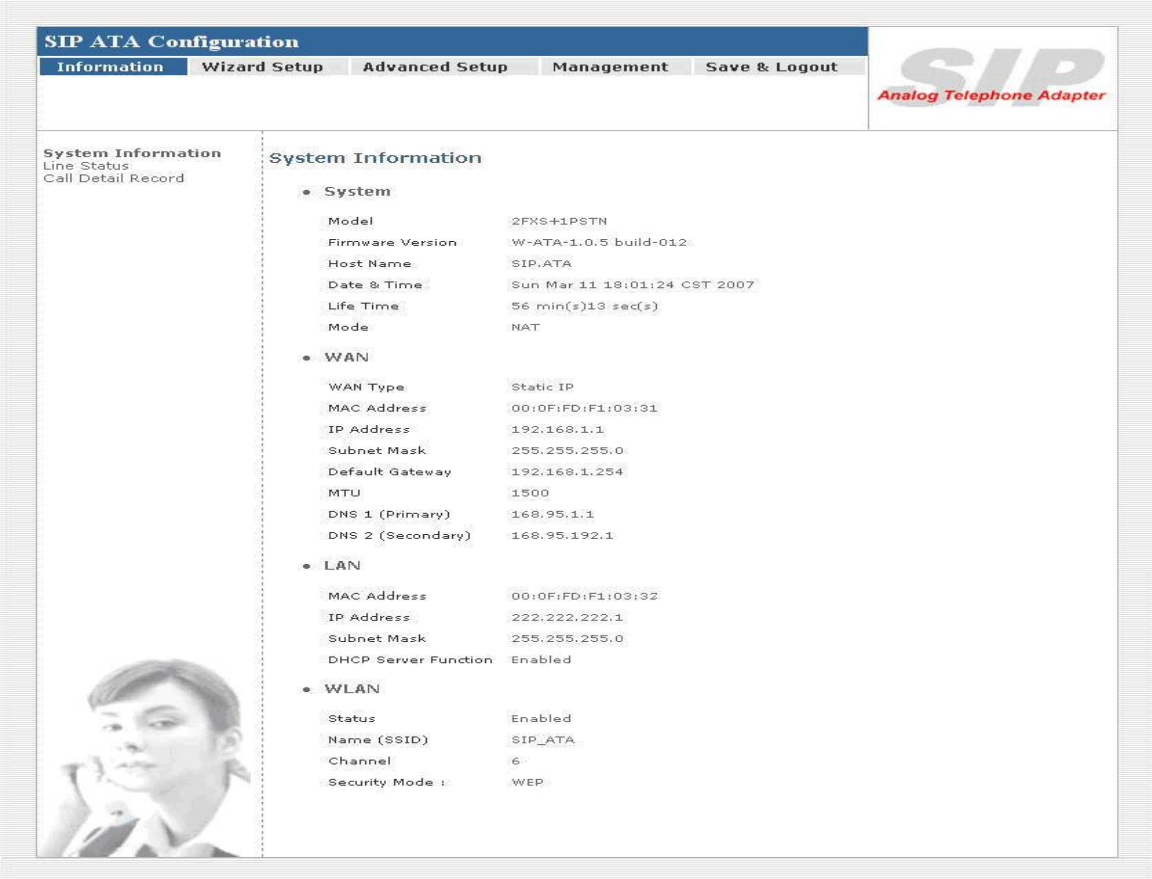
to set both low delay and high throughput.

Information

- System Information
- Line Status

6.1 System Information

Click System Information to display system status, WAN type, and LAN type. WLAN type.

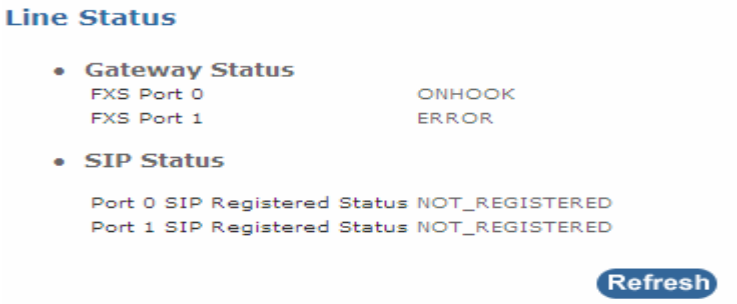


This page displays the current information for the device. It will display the LAN, WAN,WLAN (Status / SSID /Channel / Security Mode)and system firmware information. This page will display different information for you, according your WAN setting (Static IP, DHCP, or PPPoE).

If your WAN connection is set up for Dynamic IP address, there will be a Release button and Renew button. Use Release to disconnect from your ISP and use Renew to connect to your ISP.

If your WAN connection is set up for PPPoE, there will be a Connect button and **Disconnect button. Use "Disconnect" to drop the PPPoE connection and use** "Connect" to establish the PPPoE connection

6.2 Line Status



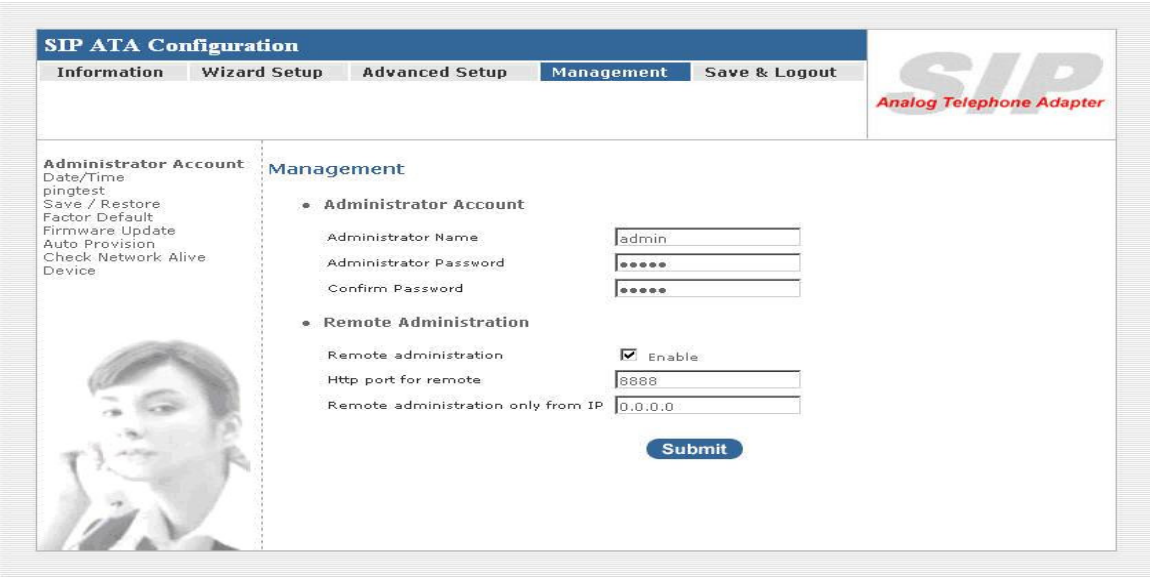
This window displays the FXS ports and SIP registered status. Click on Refresh button to retrieve the status.

Management

- Administrator Account
- Date/Time
- PING Test
- Save/Restore
- Factory Default
- Firmware Update
- Auto Provision
- Check Network Alive
- Device

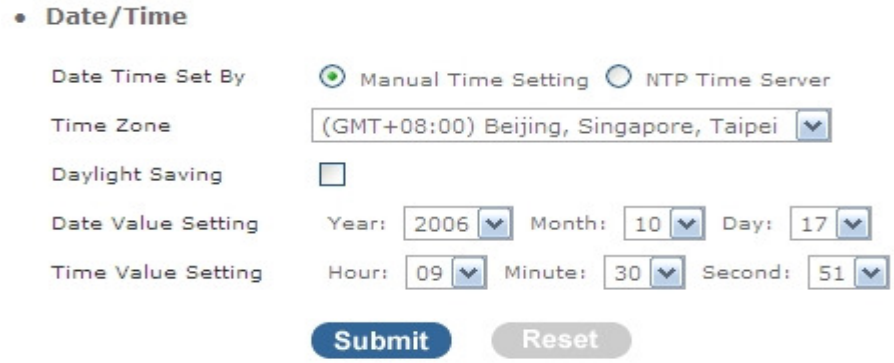
7.1 Administrator Account

The administrator account can access the management interface through the web browser. Only the administrator account has the ability to change account password.

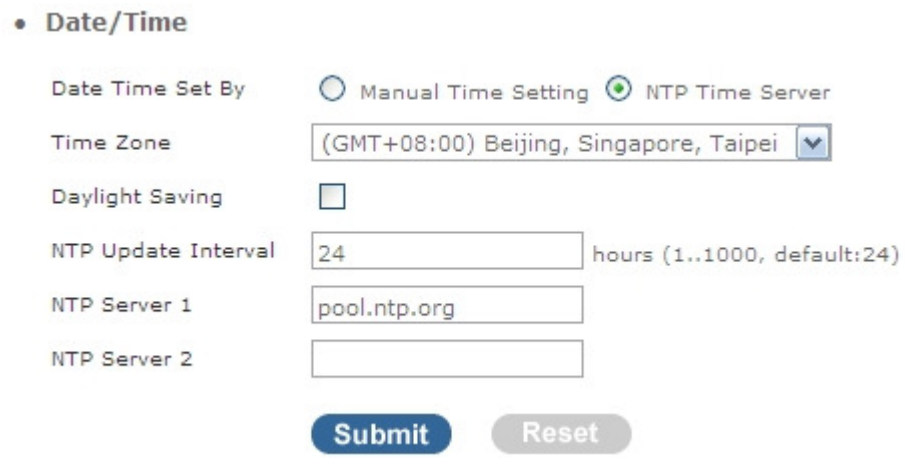


□Administrator Name - Assign a name to represent the administrator account. Maximum 16 characters. Legal characters can be the upper letter “A” to “Z”, lower letter “a” to “z”, digit number “0” to “9” and an underscore sign¡ ”_”.
The administrator name is case-sensitive. Note: the “blank” character is an *illegal character*
□Administrator Password - Assign the administrator password. Maximum 16 characters and minimum 6 characters. Mix the characters with the digits. Legal characters can be the upper letter “A” to “Z”, lower letter “a” to “z”, digit number “0” to “9” and an underscore sign”_”. The password is case-sensitive. Note: the “blank” character is an illegal character.
□Confirm Password - Enter the administrator password again. Remote Administrator allows the device to be configured through the WAN port from the Internet using a web browser. A username and password is still required to access the browser-based management interface.
□Remote Administration - Enable/Disable to access from remote site. Default setting is “Disable”.
□Http port for remote - If you allowed the access from the remote site, assign the http port used to access the ATA. Default port number is “8888”.
□Remote administration only from IP - Internet IP address of the computer that has access to the ATA. Assign the legal IP address.
Example:
http://x.x.x.x:8080 where as x.x.x.x is the WAN IP address and 8080 is the port used for the Web-Management interface.

7.2 Date/Time



□Manual Time Setting - Set up the time manually.



□NTP Time Server - Protocol used to help match your system clock with an accurate time source. For example atomic clock or a server.
□Time Zone – Choose your time zone , Default is (GMT+8:00)Beijing,Singapore,Taipei.
□Daylight Saving – Enable / Disable ,Default is Disable,time during which clocks are set one hour ahead of local standard time; widely adopted during summer to provide extra daylight in the evenings
□NTP Update Interval – Default is 24 hours , This is used to select the frequency of. NTP updates
□NTP Server 1 – Default is "pool.ntp.org",NTP Server address.
□NTP Server 2 – Default is empty.

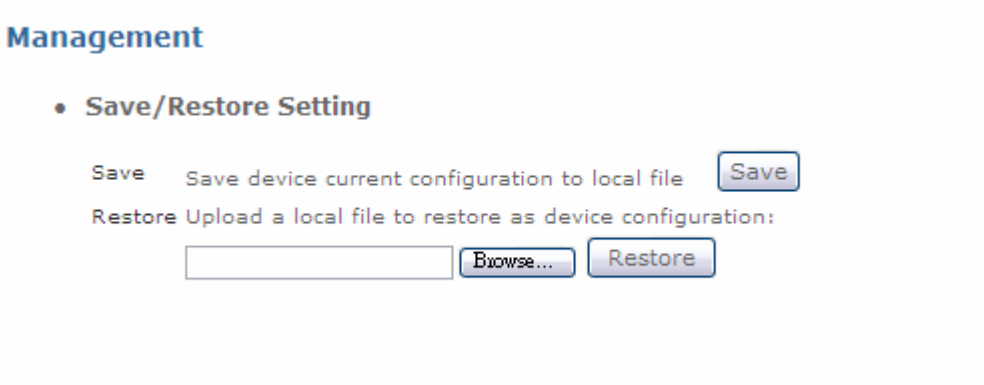
7.3 Ping Test

This useful diagnostic utility can be used to check if a computer is on the Internet. It sends ping packets and listens for replies from the specific host. Enter in a host name or the IP address that you want to ping (Packet Internet Groper) and click Ping.
Example: www.yahoo.com or 216.115.108.245

□Ping Destination - Assign a legal IP address.

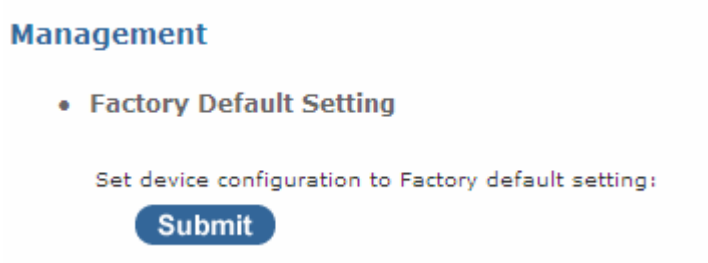
7.4 Save/Restore

All settings can be saving to a local file. Or, you can upload a local file to restore as the device configuration for the Telephony ATA.



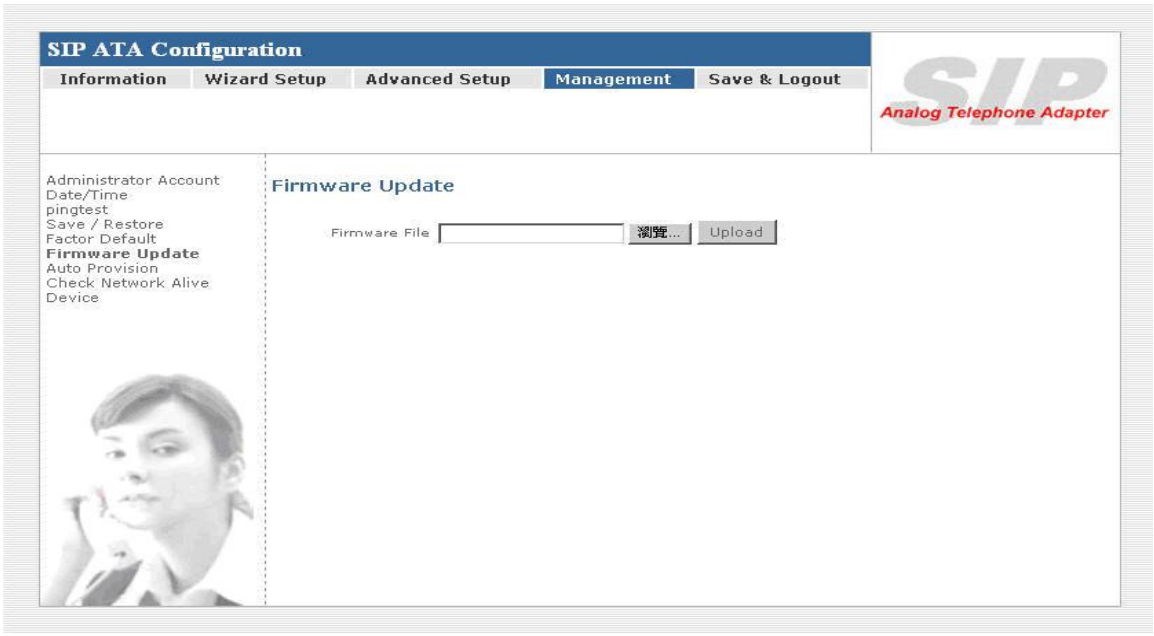
7.5 Factory Default

This function is used to restore all the parameters back to factory default setting. You can use the Save/Restore Setting (please refer to the section of 7.3 "Save/Restore¡¨) to check the factory default configuration, after you click on the **Set** button.



7.6 Firmware Update

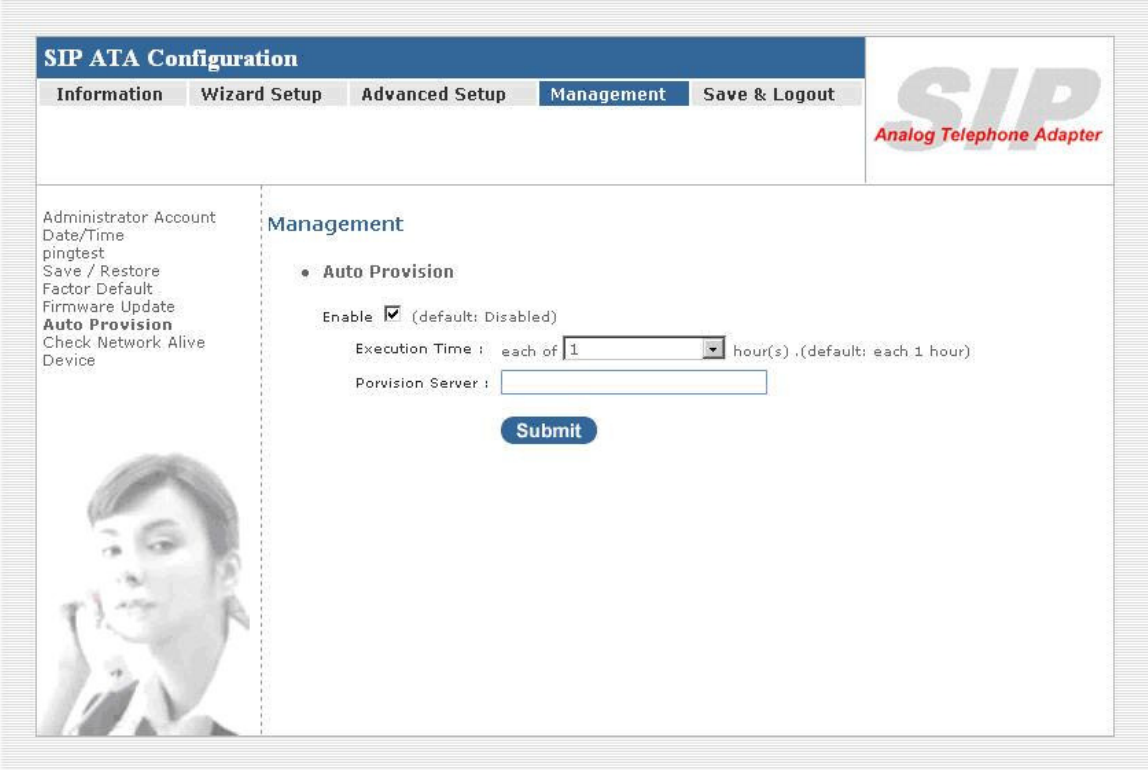
You can upgrade the firmware of the device using this tool. Make sure that the firmware you want to use is saved on the local hard drive of the computer. Click on Browse to search the local hard drive for the firmware to be used for the update. Upgrading the firmware will not change any of your system settings but it is recommended that you save your system settings before doing a firmware upgrade.



Firmware Name: select that you want to upgrade Firmware version.

7.7 Auto Provision

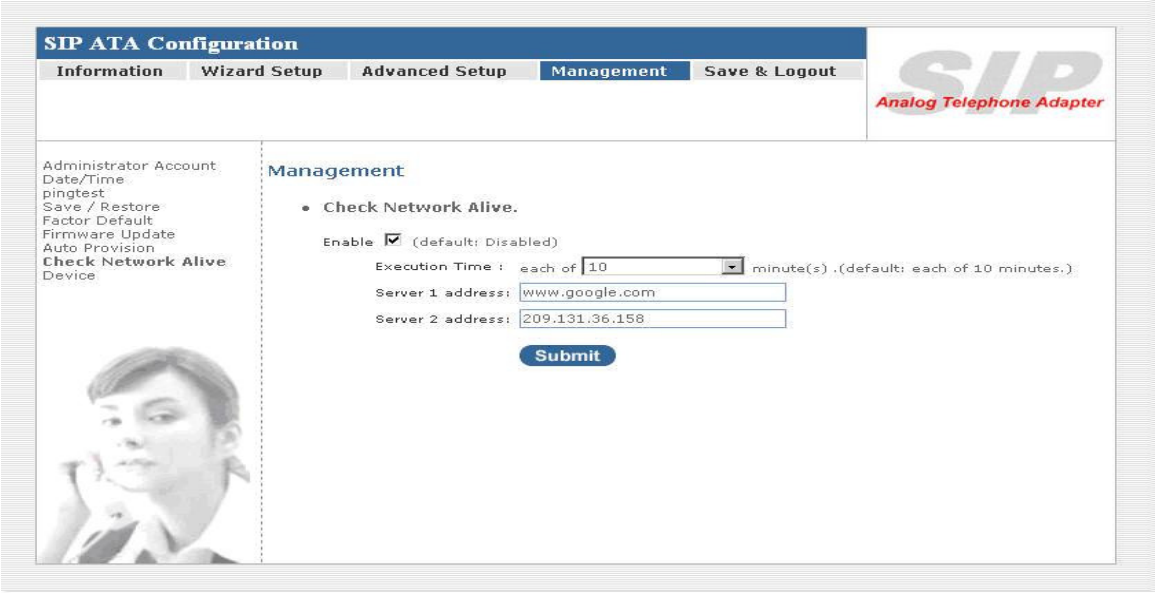
Enable or disable the auto-provisioning feature. If enabled ATA will try to download the configuration files from the provisioning server.



□Excution Time - Default 1 hour (1 to 10 hours) , ATA will try to download the configuration files from the provisioning server.
□Provision Server - Provision Server ,default is empty.

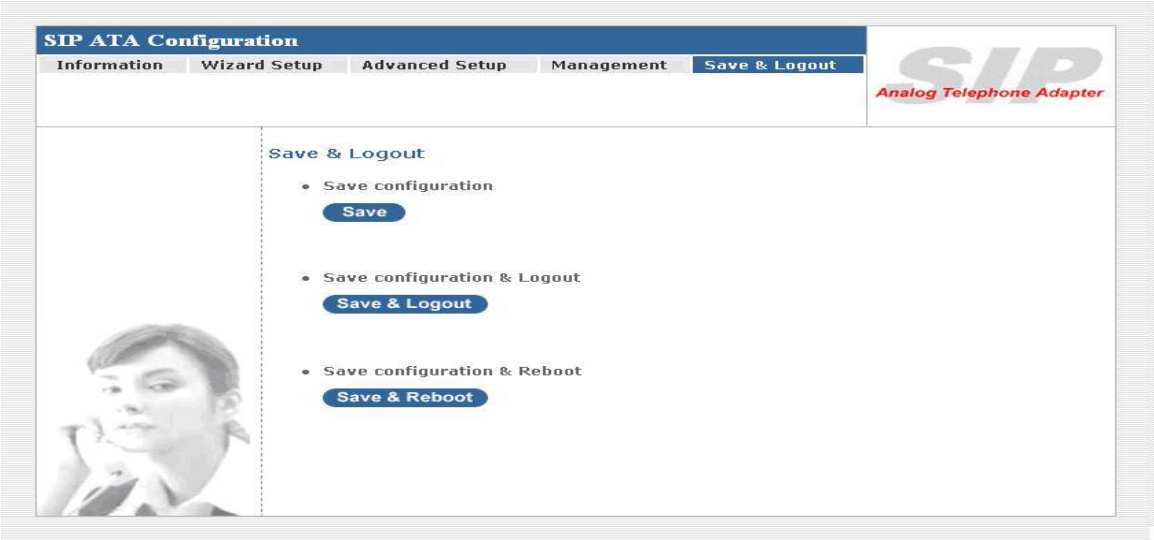
7.8 Check Network Alive

Use the Check network alive Net valid node checking security feature to allow or deny access to server processes from network clients with specified IP addresses.



□Execution Time - 5 ~ 55 min,default 10min
□Server 1 address - www.google.com
□Server 2 address - 209.131.36.158

Save & Logout

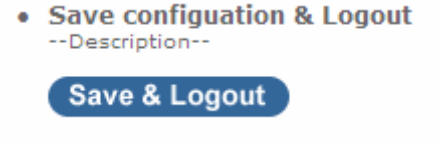


8.1 Save

Save your ATA Setting after you setting finish.

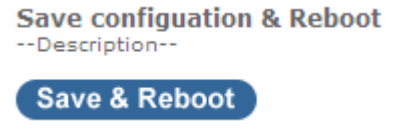
8.2 Save & Logout

If you need to logout administrator right for web-access, please click the Logout link. The web system management interface will auto-logout with 1800 sec default value.



8.3 Save & Reboot

If for any reason the device is not responding correctly, you may want to reboot the ATA system



Appendix

A - FAQ List

1. What is the default administrator password to login to the ATA? How to Login?
A: By default, default username is “admin”, default password is also “admin” to login to the router. For security, you should modify the password to protect your gateway against hacker attacks.

Default Wan Port IP Address is “192.168.1.1”, Lan Port IP Address is “222.222.222.1”.Loging Web User Interface, open the Bowser(IE/FireFox) and input IP address.

2. I forgot the administrator password. What should I do?
A: Press the **Reset** button on the rear panel for over 5 seconds to reset all settings to default factory values. Then you can use the default Username/Password to Login Web UI.

3. Why is it that I can ping to outside hosts, but not access Internet Web sites?
A: Check the DNS server settings on your PC. You should get the DNS servers settings from your ISP. If your PC is running a DHCP client, remove any DNS IP address setting. As the ro uter will assign the DNS settings to the DHCP-client-enabled PC.

4. What is the maximum number of IP addresses that the DHCP server of the gateway can assign to local PCs?
A: The built-in DHCP server can support 253 IP addresses for local network usage.

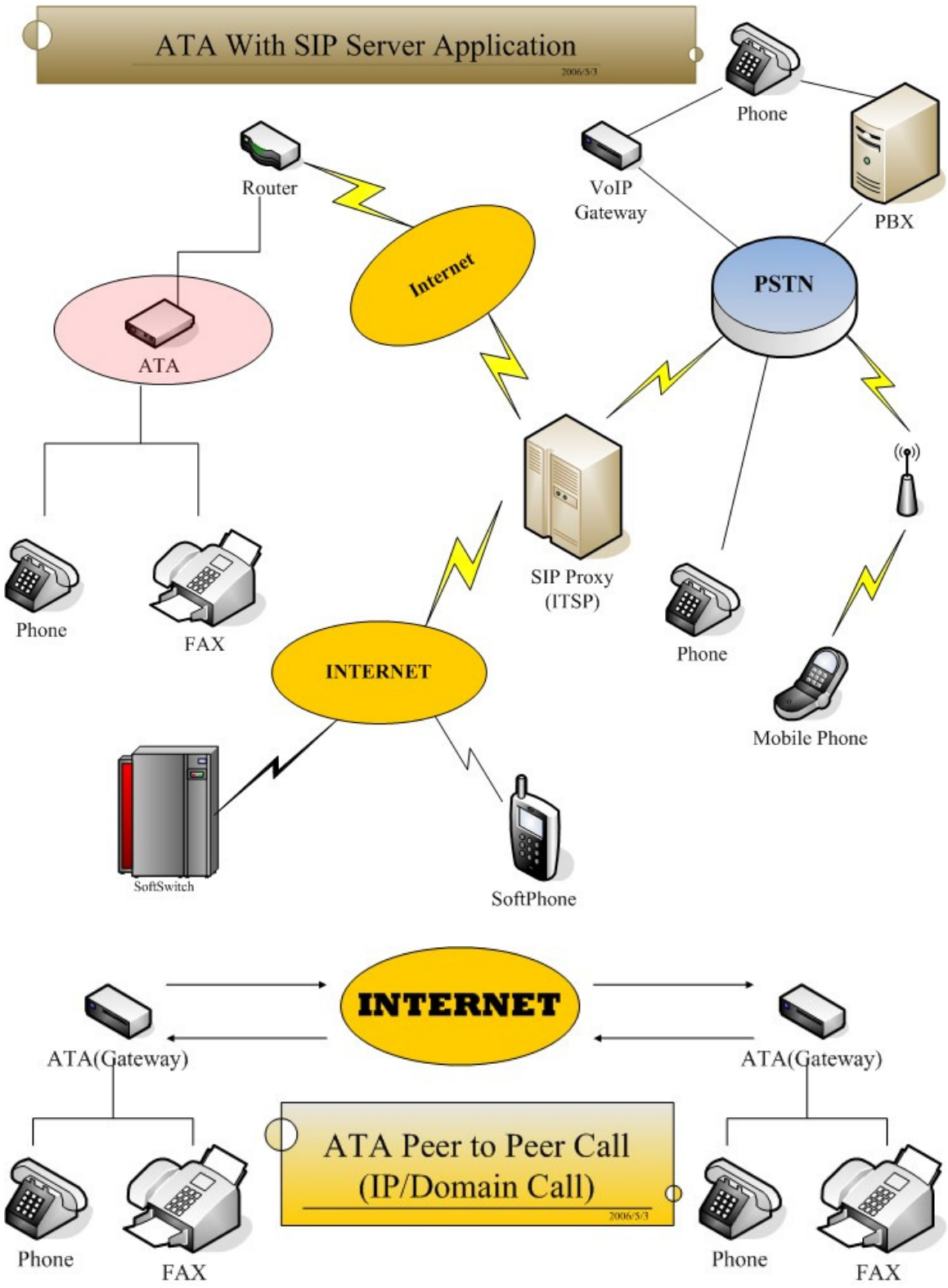
5. Why can I call out by ATA?
A: Please chick your ATA is registered SIP Proxy Server(ITSP), and chink your Internet works fine. ATA can’t make a call without Internet or SIP Account that from ITSP supply. You must have a SIP account or know the other ATA/Gateway IP/Domain Name, then you can make a VoIP call.

6. I can’t use web Interface to setting ATA, How can I do?
A: Please check you PC connect the ATA Lan port or PC and ATA with the same Subnet. If you PC aren’t at the same Subnet, you can’t Login the ATA Web interface. Else you let your ATA on Public Internet(Public IP address).

7. Why does the one way talk happen?
A: Generally, one way talk happen when use the different codec between VoIP device make call. Please check and setting the same codec, most one way talk will be solved.

8. Why can I call out when the ATA under the NAT?
A: VoIP product almost have NAT Pass through problem. By SIP, there are many NAT Pass through Function can solve 80% NAT Problem. You can choose STUN/Outbound Proxy/ Symmetric RTP to Pass through NAT, you don’ t set any other setting (DMZ/Virtual Server) by router side. If you use STUN/Outbound Proxy, you must have a STUN/Outbound Proxy Server to support. If they can’ t pass NAT, please open the DMZ/Virtual Server by Router/NAT/Firewall.

B - Scenario Application Samples


ATA With SIP Server Application
2006/5/3
Phone
Router
VoIP
Gateway
PBX
Internet
PSTN
ATA
SIP Proxy
(ITSP)
Phone
FAX
Phone
INTERNET
Mobile Phone
SoftSwitch
SoftPhone
INTERNET
ATA(Gateway)
ATA(Gateway)
ATA Peer to Peer Call
(IP/Domain Call)
2006/5/3
Phone
FAX
Phone
FAX